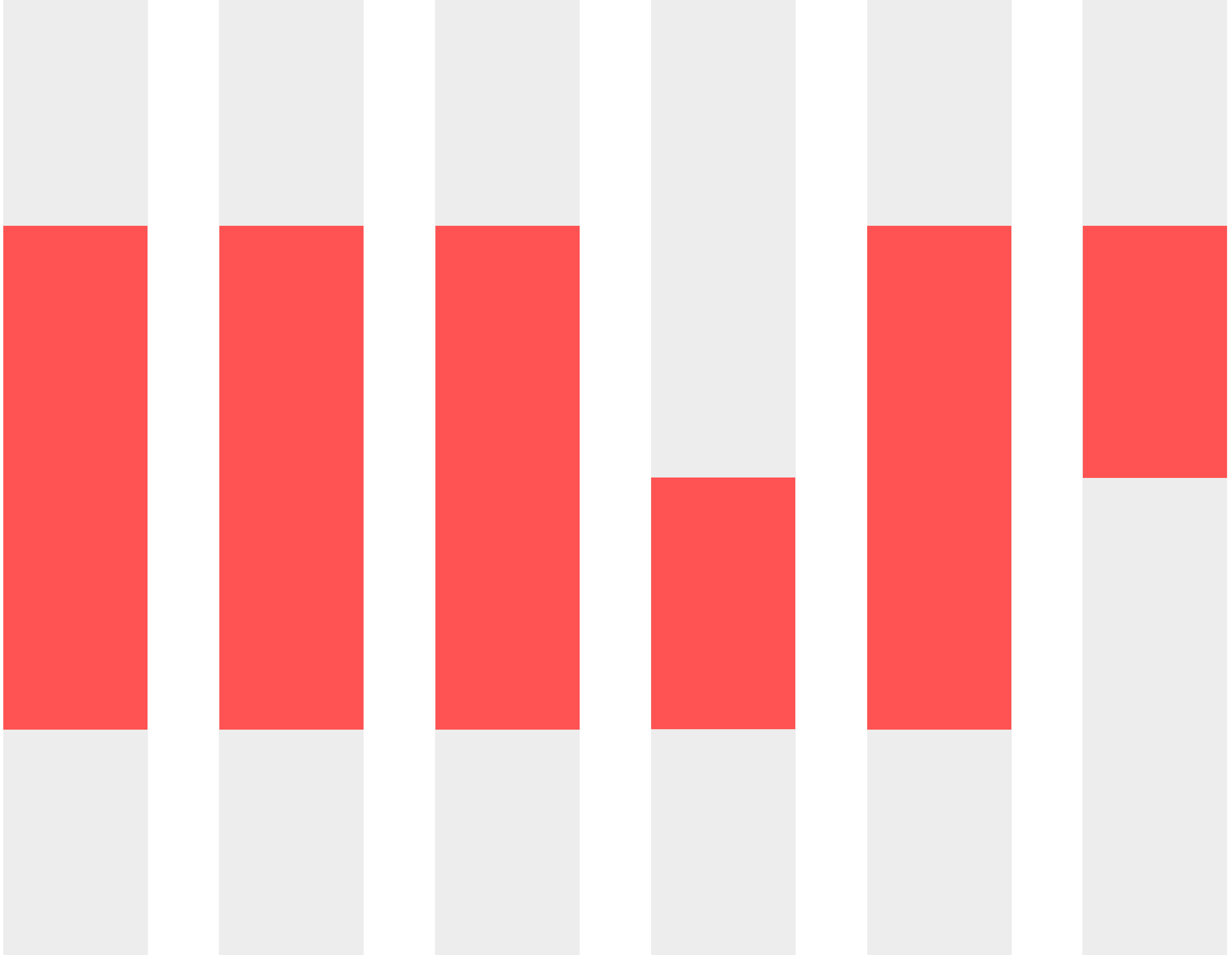


Marcin Szewczyk

My name is Marcin Szewczyk-Wilgan and I am a full-stack designer. I am professionally involved in typography and publication design and visual communication. I also specialise in automating the processing of text data.

As a certified UX designer, I create usable websites and online stores based on WordPress and Woocommerce. I manage Linux / FreeBSD systems for hosting and cyber security services.

In 25 years of work in the publishing and internet technology industry, I have gained considerable recognition among dozens of companies and institutions.

- Magazine and book design
- Desktop Publishing (DTP)
- Print and digital typography
- UX/UI design and prototype
- Websites, e-commerce systems – design and optimization
- Administration of Linux / FreeBSD systems and hosting services

CONTACT

Marcin Szewczyk-Wilgan

marcin.szewczyk@m4c.pl

+48 608 271 665

Wrocław, Poland

25 YEARS OF MY PROFESSIONAL WORK IN NUMBERS

24
layouts for magazines and trade journals

281
books made with the utmost care

41
designed and launched websites

Selected clients for whom I have completed projects

Adobe
presscom
GHELAMCO
WARSAW SPIRE
PGE
nto NOWA TRYBUNA OPOLSKA
POLSKA PRESS GRUPA
Microsoft
ringier axel springer
Politechnika Wrocławska
DZIENNIK ZACHODNI
media regionalne
Radio Opole
pfo
ON BOARD THINK KONG ecco network
POLITECHNIKA OPOLSKA
Dolnośląskie Centrum Psychodynamiczne
UNIWERSYTET SWPS
VETOS FARMA GRUPA VETOS-FARMA
BEST in LOMBOK
Uniwersytet Wrocławski
castellum
EAVPT European Association for Veterinary Pharmacology and Toxicology
Solidarność
TYCHY
Vinderen
MAZURKAS Travel Poland
echo miasta
cookiness STUDIO KULINARNE

Selected works, table of contents (click to move)

01. *Best In Lombok* magazine

Best in Lombok is a quarterly publication. Mission is to present companies (hotels, restaurants, bars, tour operators and various types of activities) that have an established market position, very good customer reviews and care for the highest level of service. The journal contains information about the most interesting places and regularly held events that can make tourists stay in Lombok more successful. The publisher, also aspire to be the broadest-distributed and controlled publishing house. Every issue is available at six Indonesian airports with direct connections to Lombok, thanks to partnership with Angkasa Pura Airports, and at 100 of Lombok's most popular tourist destinations.

Scope of work:
– design
– layout
– typography
– logotype
– desktop publishing
– pre-press

↑ Click to move to Table of Contents

Dear Best in Lombok Readers,

We are delighted to share with you the first edition of the Best in Lombok guide.

Lombok is often nostalgically compared to Bali 30 years ago. The pristine nature, friendly locals, great climate and stunning views are so rare to find in tourist destinations these days – and are what we all love and cherish about Lombok today. These are undoubtedly only some of the reasons that brought you to this emerging gem of Indonesia. Here at Best in Lombok, we want every single visitor to have the best experience possible, and to that end, we have created this publication to become your go-to reference, and once you get home, a keepsake to share with friends and family who might be thinking of traveling to Lombok.

Every quarter, we will enrich our guide with more attractions, options and information, because we strongly encourage you to travel around Lombok, whether in the form of organized trips, a rented scooter, or simply discovering the island through active recreation from the mountains to the depths of the sea.

In our guide we would like to advise you on how to spend your holiday in an active way, areas to visit, where you can count on great cuisine or cocktails, or where to just slow down and take in the scenery. We believe that the description of activities, locations, recommendations and contact information will be useful in planning your stay in Lombok. We want to show you what is Best in Lombok, and we wish you an unforgettable holiday!

The BiL Editorial Team

INSIDE

Issue 1 - September 2019

Discover **Scuba Diving**

You'll always remember your first underwater breath. **Whether you're a beginner or expert diver, Lombok is the perfect location to experience diving**, with an abundance of coral reefs and underwater sea life, including sea turtles, and the elusive and exotic mola mola, or sunfish.

Get Your PADI

If you've always wanted to take scuba diving lessons, experience unparalleled adventure and see the world beneath the waves, this is where it starts. Get your scuba diving certification with the PADI® Open Water Diver course – the world's most popular and widely recognized scuba course. Millions of people have learned to scuba dive and gone on to discover the wonders of the aquatic world through this course. To enroll in a PADI Open Water Diver course (or Junior Open Water Diver course), you must be 10 years old or older. You need adequate swimming skills and need to be in good physical health. No prior experience with scuba diving is required. Certifed divers can sharpen their skills in PADI Specialty Courses, PADI Rescue up to Divemaster level.

PADI

You Can Dive!

To sign up for a PADI Discover Scuba Diving experience, you must be at least 10 years old. No prior experience with scuba diving is necessary, but you need to be in reasonable physical health. After a short introductory dive in the swimming pool, your instructor will assist you to enter the sea and discover underwater life, not deeper than 12 m. Are you ready to try it out?

Choose your scuba paradise

Gili Islands
Three small and very popular islands located in the northwest of Lombok, called "The Turtle Capital Of The World". Signature: sea turtles, shipwrecks, drift diving, reef sharks. For all levels.

Pink Beach
In southeast Lombok, famous for its pink sand and vibrant coral reefs. Signature: pristine coral, sharks, occasional mola mola sightings.

Kuta / Gerupuk
Dive sites located east and west of Kuta, in south Lombok. Signature: rock formations, colorful coral, reef sharks, macro diving. For all levels.

Sekotong
Off southwest Lombok, and less developed, 13 small islands provide solitude when diving. Signature: macro diving, colorful corals. For all levels.

FUN DIVING

- **Senggigi** – Gili Islands – 3 dives package (for certified divers): 1,600,000 Rp
- **Kuta** – Kuta area – 2 dives package (for certifed divers): 1,300,000 Rp
- **Kuta** – Pink Beach or Sekotong (for certified divers): 1,800,000 Rp

COURSES

PADI OWD Course, 3 days
- Gili Islands: from 5,650,000 Rp
- Kuta: from 5,500,000 Rp

DISCOVER SCUBA DIVING

- Gili Islands – 2 dives: from 1,800,000 Rp
- Kuta – 1 dive: from 1,100,000 Rp

WHERE TO BOOK?

SCUBA FROGGY PADI 5 STAR DIVE CENTER
Senggigi–Kuta–Gili Trawangan
www.scubafroggy.com
contact@scubafroggy.com
Scuba Froggy – Senggigi
Scuba Froggy – Kuta Lombok
Senggigi/Gili +62 (0)878 6551 1090
Kuta +62 (0)819 1723 4986

Scuba Froggy
LOMBOK · GILI ISLANDS · KOMODO

Explore **Kitesurfing**

Kitesurfing is a challenging sport that's lots of fun from your very first try. It's a combination of sailing, windsurfing and board sports. You always need to start your kitesurfing adventure with a qualified instructor. Otherwise it can be dangerous.

Indonesia has long been considered a paradise for surfers, but it's still relatively unknown as a kitesurfing haven. During the windy months of April to September, several spots along Lombok's south coast are perfect for kitesurfing, with one of the best being Kaliantan beach in southeast Lombok. That's where you'll find Kaliantan Kitesurf. The lagoon at Kaliantan is surrounded by a reef that provides perfect conditions for learning and riding. For advanced kiters, there's the option of a 7 km downwinder along the coast.

Kaliantan Kitesurf is IKO certified, and all lessons meet IKO standards. The school is equipped with the latest Liquid Force gear, and because it's located in a pristine and remote area, you'll find serenity and relaxation after your adrenaline rush on the water. After your session, take a shower, use the facilities and grab a refreshing drink or cold beer.

The most convenient place to stay for Kaliantan kiters is Ekas Breaks Resort, just a few minutes away. There, you'll find special offers as a kitesurfing guest. Just ask about the "Kite Stay" package.

WHERE TO START?

Kaliantan Kitesurf – the school connected with The Playground Kuta – is a dream place for both riding and learning. Its sunny, uncrowded and protected location is the perfect stage to learn this exhilarating sport.

THE WINDIEST TIME

The windy season starts here in late April and lasts until October. Wind usually picks up from early afternoon or even late morning in the peak of the season so you can kite most of the day. The average wind speed is 16–23 knots.

KITESURFING COURSE

- **6h package**: for beginners or intermediate riders: 5,500,000 Rp
- **10h package**: for beginners (prepare to become an independent kiter): 9,000,000 Rp

KITESURFING LESSON

- **2h lesson**: for all who want to improve or refresh their kitesurfing skills: 2,000,000 Rp
- **session**: for those who finish course but do not feel comfortable alone in the water: 1,400,000 Rp

All lessons and courses include full gear and supervision of qualified instructor. We offer only private lessons (1 student + 1 instructor).

WHERE TO BOOK?

THE PLAYGROUND KUTA
www.lombokplayground.com
+62 (0)811 3906 566
and Scuba Froggy offices in Senggigi

ThePlayground
ACTION SPORTS · WATER SPORTS · CLUB

Snorkelling Tours

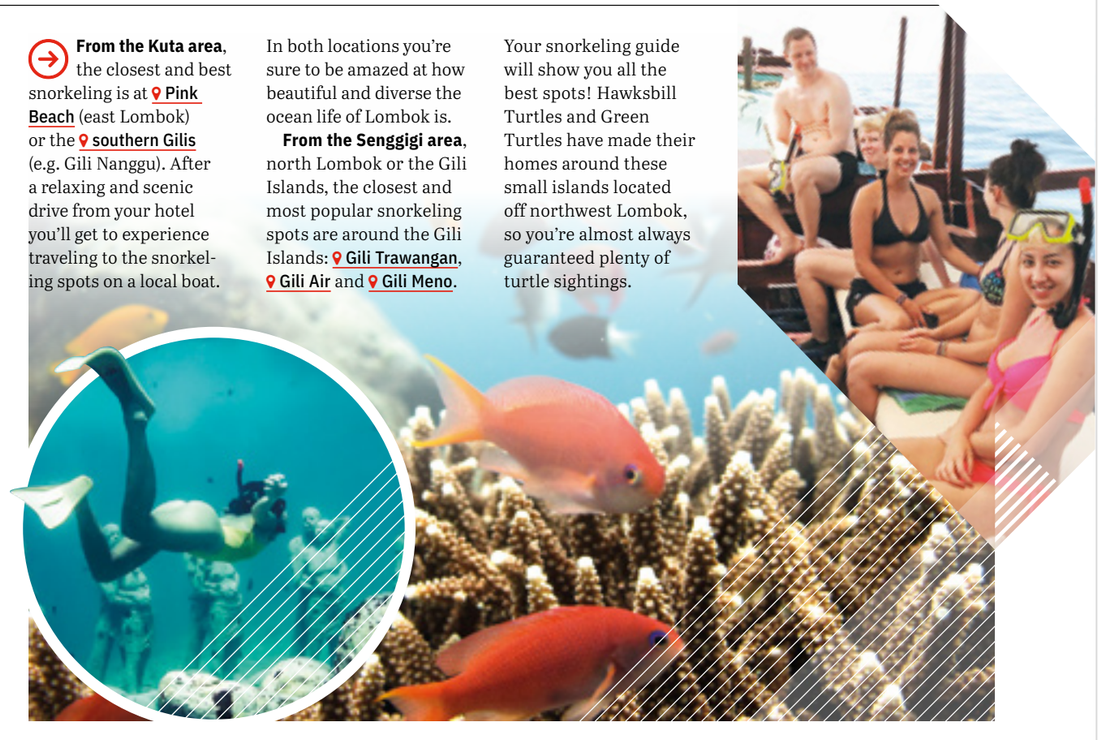
Lombok offers non-scuba divers plenty of great opportunities to explore abundant sea life in crystal clear waters. **No previous experience is required to discover Lombok's hidden treasures with just a snorkel and mask, from sea turtles and coral gardens to a world-class diversity of fish**. It's a chance for the whole family to create life-long memories.

From the Kuta area, the closest and best snorkeling is at **Pink Beach** (east Lombok) or the **southern Gilis** (e.g. Gili Nanggu). After a relaxing and scenic drive from your hotel you'll get to experience traveling to the snorkeling spots on a local boat.

In both locations you're sure to be amazed at how beautiful and diverse the ocean life of Lombok is.

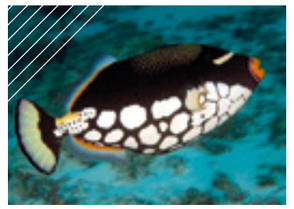
From the Senggigi area, north Lombok or the Gili Islands, the closest and most popular snorkeling spots are around the Gili Islands: **Gili Trawangan**, **Gili Air** and **Gili Meno**.

Your snorkeling guide will show you all the best spots! Hawksbill Turtles and Green Turtles have made their homes around these small islands located off northwest Lombok, so you're almost always guaranteed plenty of turtle sightings.



You can meet these species and more while snorkelling

Angelfish



Clown Triggerfish

Sweetlips

Map Puffer

Yellow Boxfish

Hawksbill Turtle

Cuttlefish

Titan Triggerfish

Green Turtle

Moorish Idol

BE A RESPONSIBLE TOURIST!

1. Don't touch turtles and avoid fish feeding sessions.
2. Don't touch or step on corals.
3. Don't collect sea shells from the ocean or the beach.
4. Don't stay close to the engine.
5. Wear a life jacket if you are not a confident swimmer.
6. Refuse plastic straws and bags.
7. Use coral friendly sunscreens.
8. Use sun protective clothing while snorkelling.
9. Support local clean-up actions.

POPULAR SNORKELLING PROGRAMS

- **Gili Islands from Senggigi**: 600,000 Rp/pp (incl. boat, equipment, guide, drinks, snack, lunch box, Autore Pearl Farm tour; 3 spots around Gili islands); + 50,000 Rp for car transportation
- **Pink Beach from Kuta** (min. 2 persons): 900,000 Rp /pp (incl. boat, guide, equipment, water, snack, lunch box) + 100,000 Rp for car transportation
- **Gili Nanggu from Kuta** (min. 2 persons): 900,000 Rp / pp (incl. boat, guide, equipment, water, snack, lunch box) + 100,000 Rp for car transportation

WHERE TO BOOK?

SCUBA FROGGY SENGGIGI

contact@scubafroggy.com
+62 (0)818 0528 8923
+62 (0)878 6579 8117

Scuba Froggy

Family & Friends **Water Games**

With all the action sports Lombok is perfectly suited for, why choose just one? It's easy to combine your favorite pursuits to get your adrenaline pumping. **From kayaking and wakeboarding off the northwest of Lombok, to scuba diving and kitesurfing in the popular south, creating an experience to remember is easy.**

Active Travelling – Kids Included

Sure, many travelers long for lazy days pouring over a book on a sun lounger on the beach, and there are plenty of opportunities for that in Lombok. But, after a few days, cabin fever might set in, especially for kids. Many adventure sports are perfectly suitable for children, or can be tailored towards kids' and teenagers' needs. Whether dialing down on the speed, or hiring a dedicated professional instructor, any activity can be appropriate and fun for young travelers.

Water Games – Senggigi or Kuta

Experience an unforgettable two hours with access to all the water sports toys and your own private instructor. These tours, staging from the beautiful sand beaches at Sheraton Senggigi Beach Resort in northwest Lombok, or Novotel Lombok Resort & Villas in Kuta on the south coast, are perfect for people who want to do it all with a combination of adrenaline-pumping activities such as jet skiing, wake boarding and donut riding, and more relaxing pursuits like stand up paddling and kayaking. The locations, with views of either the spectacular coastline of northwest Lombok or the secluded bay and famous Seger break in the south provide perfect backdrops for an exhilarating and unique experience.

Must try!

Groups of 2-8 people can enjoy all these water sports with minimal instruction, or a full lesson, during the duration of the adventure.

DONUT

This is one of the most exhilarating activities to do with friends and family. Hanging on to the donut while being towed behind a speed boat or jet-ski, the twists, turns, bumps and jumps will surely get your heart rate up. Max 2 people at a time.

STAND UP PADDLE (SUP)

An offshoot of surfing, done standing on an oversized surfboard and propelling forward with a paddle, SUPing is easily enjoyed by first-timers without much instruction. **SUPers can explore the ocean and enjoy Lombok's tropical scenery from the seaside.**

KAYAK

Solo or tandem, kayaking can be both relaxing and great physical exercise, for paddlers of all ages. **It's easy to grasp the technique and sitting down in the kayak makes it suitable even for the youngest of explorers.**

WAKEBOARD

Like snowboarding but on water, wakeboarding is a challenge, but for those who try it, also addictive. Be prepared for some thrills and spills. One person at a time.

SENGGIGI OR KUTA WATER GAMES

- **For who?** Families and friends, min. 2 pax
- **Duration:** 2 hours
- **Price:** 1,100,000 Rp/pp
- **Included**: transportation in Kuta or Senggigi, all equipment, instruction, drinking water, towels and snacks.
- All activities except wakeboarding and donut ride are suitable for all ages.

WHERE TO BOOK?

THE PLAYGROUND KUTA
+62 (0)811 3906 566

SCUBA FROGGY SENGGIGI
+62 (0)818 0528 8923
+62 (0)878 6579 8117

Scuba Froggy | ThePlayground

Down The **River**

Rafting is not a high-performance sport. It does not require any special skills or physical fitness, yet you experience all the thrills and adrenaline of an extreme sport. All you need is a helmet, life vest, comfortable clothes, and a bit of moxie.

Your rafting guide will teach you where to sit, how to use the paddle and what to look out for in the river, and off you go!

One of the best rafting routes starts in Lingsar, on the Jangkok Lingsar River in West Lombok. After picking up your gear, you'll drive through rice fields and jungle to the starting point where your raft and guides meet you. The exhilarating 2-hour, 5-km trip on the river will take you through villages, untouched wilderness and, if you're lucky, a few kids splashing in the river, or ladies doing the washing the traditional way. Along the way, the adventurous have the chance to dive into rock pools, and those a bit more faint-at-heart can relax in the natural ponds and caverns.

During rainy season, each raft can accommodate six persons, plus a guide, or during the dry season, 3 persons, plus the guide.

If you still have energy, on the way back, visit **Lingsar temple**, a symbol of harmony between Balinese Hindu and Sasak Muslim traditions. Also, don't miss the beautiful and imposing **Timponan waterfall**.

For the **Kids**

It's almost as if Lombok was designed specifically for kids. With its vast sand beaches, endless oceans with an abundance of colors and sights, and lush tropical nature, it's a natural playground. But even after young travelers have had their fill of play in nature, there are plenty of options for fun activities for all ages.

Surfing

South Lombok is perfectly suited for young beginners or groms to get their feet wet in a safe and suitable setting. The waves at Selong Belanak, in south Lombok, break over the sand right onto the beach, providing perfect conditions for learning and advancing skills – all while parents can relax on a sunbed on the beach and watch the progress. For slightly more confident young surfers, Tanjung Aan and even Gerupuk can be suitably challenging, yet still safe waves with an instructor.
Ozi Lombok: +62 (0)853 3876 3536
Sasak Soul: +62 (0)853 370 0970

Bubblemaker

Bubblemaker is as fun as it sounds – a chance for kids to blow bubbles by scuba diving. Children at least 8 years old can use scuba gear to breathe underwater and swim around in shallow water. Kids must be comfortable in the water, but no prior experience is necessary. They take their first breaths underwater in water shallower than 2 meters, under PADI Pro supervision. The unique program is available in Novotel Resort in Kuta and Sheraton Senggigi, powered by **Scuba Froggy Dive Center**.
scubafroggy.com

Go Wild

Lombok Wildlife Park, a scenic 45-minute drive north of Senggigi, and a 2-hour drive from Kuta, is a small wildlife park that boasts a diverse 50 species of animals, including elephants, hippos, orangutans, reptiles and many birds. Many are rescue animals and all are cared for by a dedicated professional team.
lombokwildlifepark.com

Slip & Slide

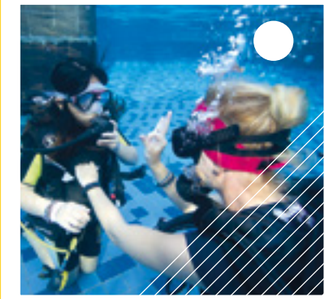
Kura Kura Family Entertainment Waterpark in central Mataram is a wet haven for the kids, with several pools, climbing structures, fountains, slides and a playground. A restaurant, billiard tables and plenty of space for the adults to relax make it easy to spend a whole day there.
+62 (0)370 616 0474

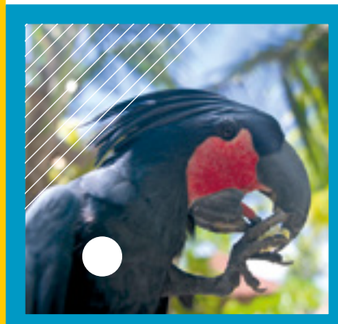
Shop & Play

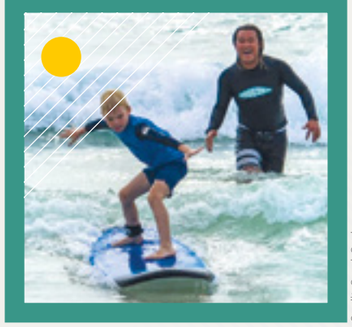
Both malls in Mataram offer hours of fun for kids. On the top floor at Epicentrum, the Time Zone arcade entertain the older kids, while the Time Zone play land lets the younger ones burn energy in a safe jungle-gym setting. In the basement, the youngest of visitors can explore tactile areas, jump in the ballpit and ride cars in the Happy Family play area. At Transmart Carrefour shopping mall, the entire top floor is a dedicated kids zone, with many arcade games, train rides – and even an inside/outside rollercoaster!
lombokepicentrum.com
carrefour.co.id

Cinema

Want to get out of the sun for a bit? Head for some big-screen entertainment in Lombok's big city, Mataram. Both Epicentrum mall's Cinema 21 and Transmart Carrefour shopping mall's CGV Cultureplex show the latest Hollywood blockbusters in 2D, and 3D when available, with several screens and VIP screening rooms, so buy some popcorn and while away a few hours.
21 Cineplex at Epicentrum:
21cineplex.com
CGV Cultureplex at Transmart Carrefour: cgv.id







Credit: Sasak Soul

Home Away From Home

Imagine stepping off the plane in Lombok, your cheeks instantly getting rosy from the warm, tropical air. After you roll your luggage from the carousel, a friendly face meets you and helps you with your bag, as you walk toward the air-conditioned car that will shuttle you the quick 20 minutes to Novotel Lombok Resort & Villas in Kuta, on the south coast of Lombok.

As you step out of the car, it's like you've been transposed to a tropical oasis, removed from any traffic, noise or stress. Strolling from your accommodation to the restaurant, spa, pool or your own private beach berugak (traditional Lombok hut), you meander along the winding paths between lush palm trees and colorful hibiscus, with the sound of the ocean the only thing breaking the silence. This will be your home away from home in Lombok.

Keep the little Boss busy

Kids are never bored at Novotel Lombok. Whether monkey feeding, climbing, swimming, horseback riding, stand-up-paddling, playing volleyball or digging in the sand, kids of every age and interest stay busy. The shaded and supervised Kids Club provides the youngest guests with daily activities ranging from bracelet making and kite flying to arts & crafts and sand castle building. Located right outside Kids Club, the outdoor playground is a real-life beach jungle gym with swings, climbing structures, a swinging bridge and more. In the resort's dedicated kids pool with shallow and deep areas, complete with slides, bubbles and fountains, kids and kids-at-heart splash for hours.

CHOOSE YOUR STYLE

With both rooms and villas, all with AC, and all the amenities you'd expect, you're sure to find a comfortable place to call home.

Rooms

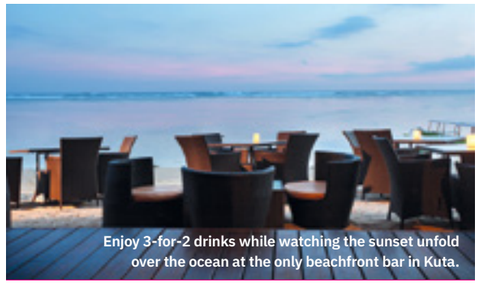
- ***Superior King/Twin*** – on the 2nd and 3rd floors with relaxing garden views
- ***Deluxe Terrace King/Twin*** – on the 1st floor with your private terrace to relax and take in the views of the lush gardens
- ***Family Rooms*** – perfect for families or groups, with two separate bedrooms and two en suite bathrooms with showers.

Villas

- ***Private Sasak Villa*** – for ultimate seclusion, with a private garden and terrace and plenty of space.
- ***Garden Pool Villa*** – when you long for privacy, and social time, a Garden Pool Villa is just right.
- ***Private Pool Villa*** – dip into your own private pool straight from your secluded villa, completely enclosed and separate from the rest of the world.
- ***Private Family Pool Villa*** – with two bedrooms, a bathroom with shower and separate bathtub, and a completely private pool and garden, you'll never want to check out.

The best of all worlds

Start your day right at the generous breakfast buffet in the open-air Spice Market restaurant, with spectacular views of the white-sand beach and turquoise waters at Bau Nyale beach. With all your western favorites; Asian specialties; pancake, waffle and egg stations; healthy smoothie bowls to order; homemade breads and pastries; oodles of fresh tropical fruits; fresh juices and much more, you'll want to linger for hours. If you're in luck, the working cows Good and Morning groom the beach and stop for photo opportunities while you're sipping your foamy cappuccino.



Enjoy 3-for-2 drinks while watching the sunset unfold over the ocean at the only beachfront bar in Kuta.

When you've worked up an appetite again, Spice Market will have transformed into a beachfront dinner venue. With themed buffet dinners, a la carte dining, and entertainment ranging from live acoustic music to local Sasak stick fighting rituals and dancing, you'll have a delicious and entertaining experience every evening.

Pamper your body & soul

At In Balance Spa, the attentive massage therapists soothe travel-weary, sun-kissed, and aching bodies, with tailor-made treatments for every need. The signature 60- or 90-minute Sasak Massage melts away any stress or tension, leaving guests in a relaxed and rejuvenated state of mind and body. Meanwhile, La Beauté salon focuses on those sun- and saltwater-frizzy locks, with rehydrating hair spa treatments, haircuts and styling by professional hairstylists.

Romance is in the air

The way to your loved one's heart is with a customized 7-course candle-lit Romantic Dinner in your private, intimate beach hut. Your dedicated staff attends to anything you need, all while giving you the privacy to feel like you're the only guests at the resort.

If elevating your adrenaline and getting a workout are on your holiday list, Novotel Lombok has it all: scuba diving, stand-up-paddling, jet-ski riding, wakeboarding, kayaking, horseback riding and more.

Best For Lunch

When a morning of exploration and activity, and the heat of the day, has you feeling drained, a sumptuous and energizing meal is in order, regardless of where you might find yourself. Luckily, Lombok boasts an abundance of options for lunch, from simple local warungs, to high-end cuisine in luxurious settings.

Hamburgerya | **Whether you're famished or just feeling like a snack, beeline to Hamburgerya, created with a love for its world-famous buns.** The menu features nine homemade buns (including gluten-free), with a variety of burgers in-between, from the classic beef, to duck, chicken, crispy mahi-mahi, and the vegetarian falafel option. Each of the burgers has a carefully composed set of sauces and toppings that make each dish have a unique taste. Try Chef's signature, The Avokadegg (beef) or The Green Fella (vegetarian) and pair with delicious sides such as homemade loaded fries with truffle oil & grated Parmesan. Delivery service available.

Prices: hamburgers 80,000-130,000 Rp, large beer 49,000 Rp
Open: 11 am–11 pm
Contact: +62 (0)877 5000 7494

Hamburgerya, Senggigi, Jl. Raya Senggigi (above Pasta Pojok)

Kenza | **Embodying island living, Kenza is openness and inclusivity - a place where all are welcomed and served with love, at any time of the day, with health-conscious food in a relaxed tropical space.** Famous for its unique coffee that is a blend of four different varieties, yet is 100% Indonesian, and baristas all trained by an expert Australian barista coach, Kenza excels in more than coffee. Suitable for all dietary preferences and needs, Kenza's menu includes vegan, vegetarian and gluten free options, including vegan green wrap, Kenza-style Spanish tortilla and tuna tartar. With an "East Meets West" concept, it also serves traditional Indonesian dishes like nasi campur, as well as western favorites like chicken parmigiana – sourced with local produce.

Prices: food 50,000-75,000 Rp, beers start at 35,000 Rp, cocktails average 80,000 Rp
Open: 7:30 am-10 pm
Contact: +62 (0)852 3849 8760

Kenza, Kuta, intersection Jalan Raya Kuta/Jalan Mawun

Laut Biru | **Directly on the famous Selong Belanak beach, Laut Biru Bar & Restaurant has been designed to blend in with the beautiful landscape, with driftwood taken directly from the beach, combined with blue hues on the floor and fresh, white walls.** This makes for a beautiful setting for you to relax with your meal while taking in the surf and white-sand beach in front of the restaurant. If you're in luck, the picture-perfect roaming buffalo herd will traverse the beach right in front of you. On Saturday evenings, enjoy the Beach BBQ, come for the Sasak Night on Wednesdays or enjoy live music all Sunday afternoon. To complement the ocean waves, the Ginger Martini and Beach Burger are a perfect combination.

Prices: starters from 42,000 Rp, mains from 52,000 Rp, beers from 29,000 Rp, cocktails from 85,000 Rp
Open: 8 am - 9 pm, daily
Contact: +62 (0)821 4430 3339

Laut Biru at Sempiak Villas, Selong Belanak – secure parking provided

Nautilus | **Located on the beach with first-row views of the crystal clear waters, Nautilus restaurant, at Gili Asahan Eco Lodge off the southwest corner of Lombok,** serves a large variety of dishes, drinks and homemade desserts inspired by fresh ingredients and traditional recipes. Enjoy a fresh, seafood-based menu with an Italian twist, popular local dishes and a variety of vegetarian, vegan and gluten-free delights. The Nautilus kitchen combines seasonal ingredients sourced at local markets with imported goods to make your culinary experience a unique and unforgettable one.

Prices: Italian wine, bottle 480,000 Rp, spaghetti vongole 85,000 Rp, pizza 70,000-90,000 Rp, gado gado 65,000 Rp
Open: 7 am–9:30 pm
Contact: +62 (0)813 3960 4779

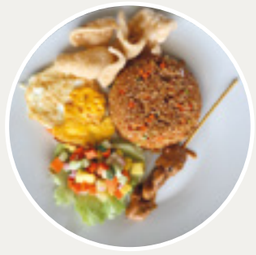
Nautilus at Gili Asahan Eco Lodge & Restaurant, Gili Asahan

Best Warungs And Local Food

Warungs are small family-owned cafés or restaurants, and are ubiquitous throughout Indonesia, and Lombok is no exception. **You'll find warungs seemingly everywhere – in the cities, towns and down to the smallest of rural villages**.

Often attached to the front of a family's house, warungs serve as gathering spots and places to share some local gossip, and eat quick, cheap and simple meals. Many warungs also take the form of small convenience stores that sell snacks, bottled drinks, cigarettes, and candy. Each warung has its own style and often serves a certain type of food, or dishes from a specific place, such as Warung Nasi (rice and simple Indonesian dishes), Warung Tegal (Javanese food originally from Tegal village in Java), Warung Padang (from Padang in West Sumatra) and Warung Kopi (coffee shop serving simple snacks).

On this page are some selected eateries to get you started on your journey to eat your way through Lombok, one local food at a time.



Senggigi

Warung Menega

Located in Batu Layar, this spacious beachside warung offers the chance to pick your fresh seafood from the fish tanks on site. Other specialties include king prawn and squid grilled over coconut shells, served with rice and water spinach.

Batu Layar, south of Senggigi

Warung Amalia

A tiny family-owned warung where you can find fresh grilled fish, king prawns and many types of salads and soups – and even a few Italian dishes.

Senggigi, near Art Market

Warung Plaza

Here, fresh Indonesian food is always presented in the glass case outside, which you can take by yourself, or ask for recommendation for the specialty of the day. Step into the air-conditioned space and cool off with some cheap eats.

Central Senggigi, opposite Sahara Club

Kuta

Warung Fishbones

Pick the fresh lobster, squid, fish, shrimp or other seafood of your choice, and they'll grill it up right in front of you. Combine your fresh seafood with their plecing kankung (spicy water spinach) and some rice, and you have a delicious meal.

Central Kuta, across from Billabong

Warung Turtle

Right on the beautiful Tanjung Aan beach, Warung Turtle serves a broad menu of Indonesian classics and simple western dishes, as well as beer. Choose to sit in the covered restaurant, or in your own berugak or under an umbrella on your sun bed.

Tanjung Aan beach, ca 15-minute drive east of Kuta

Bakso Solo

This recently opened eatery, located on the bypass road, serves a variety of soups, noodles and rice dishes, in an open-air but covered restaurant. Cheap, easy and frequented by local workers, Bakso Solo is worth the trip.

Jalan Pariwisata, leaving Kuta toward Sengkol, near the roundabout with the surfer statue

Lotus Mandalika

Recently opened in the brand-new Mandalika Bazaar, this warung serves a mix of Balinese, Lombok, Indonesian and western dishes – even Chicken Cordon Bleu, and Wienerschnitzel.

Mandalika Bazaar, near the large mosque and Kuta beach

Best For Sunset

There's a distinct romantic feeling and relaxing ambiance about the vibrant, pastel-hued sunsets in the tropics, and Lombok's west-facing spots don't disappoint. **Grab a cocktail, find a comfortable seat, order some munchies and take in nature's spectacular show**.

ASTON SUNSET BEACH RESORT · GILI TRAWANGAN

Aston Sunset Beach Resort | Venture off mainland Lombok and spend the day and night on famous Gili Trawangan, and Aston Sunset Beach Resort. The Aston Sunset Beach Resort is well-known for its perfect sunsets and breath-taking views of Bali's Mount Agung from the hotel's beach-front. Sip on cool drinks and cocktails while taking in the stunning sunset show. After happy hour (5-7 pm), enjoy watching films under the stars. Aston Sunset Beach Resort Gili Trawangan is one of many reasons to move from Lombok even for just a night or two.

Prices: affogato 43,000 Rp, shake 45,000 Rp, cocktails 91,000 Rp, small beer 58,000 Rp

Open: lunch 12 am–3 pm, dinner 5 pm–10 pm

Contact: +62 (0)878 6410 6535

Aston Sunset Beach Resort, Jl. Pantai, Gili Trawangan

Senja

Senja at Sheraton Senggigi Beach Resort | Enjoy the signature beachfront Indonesian dining experience with tables inside and out, on the edge of the blue waters off Senggigi Beach. With its magnificent panoramic view, Senja beach restaurant provides a sunset show over the ocean to the west – together with culinary delights that include Chef's Signature Lombok Food Journey. This romantic setting is the perfect spot for sharing special moments.

Prices: cocktails from 50,000 Rp, small beer from 50,000 Rp, large beer from 80,000 Rp

Open: 11 am–11 pm

Contact: +62 (0)370 693 333

Senja at Sheraton Senggigi Beach Resort, Senggigi, Jl. Raya Senggigi Km. 8

El Bazar – A Kuta Original

In 2014, El Bazar's owner arrived in Kuta, Lombok, on holiday. Completely inspired by the island's wildness, people, and sense of adventure, he went to Mawi beach to surf and spear fish for dinner on his very first day. The fish at Mawi were plentiful, to the point where the island's newcomer was able to barbecue enough food to feed an entire beach of people. He did the very same thing on his second day on the island.

Serendipitously, word came from a local restaurant owner that there was real estate available in Kuta. By his third day in Lombok, this visitor made a purchase for the space that would eventually become El Bazar, right in the center of town. El Bazar grew slowly, out of a simple desire to serve genuine food from its owner's Mediterranean home. Community support and engagement helped El Bazar gain traction in Kuta, and continued empowerment of local groups is a core priority. With this backstory, as well as a commitment to quality and consistency, El Bazar has become one of the most established and recognizable venues on the island.

El Bazar turned 5 years on September 2, 2019! Thanks to its focus on always putting its guests first, as well as constantly finding meaningful ways to contribute and give back to the local community, El Bazar has flourished and has become a mainstay in the local fabric of Kuta.

What's unique about El Bazar?

El Bazar humbly welcomes its guests for a completely unique, Mediterranean dining experience. Guests are treated as family, with all cuisine prepared from the heart, using the best available, authentic ingredients.

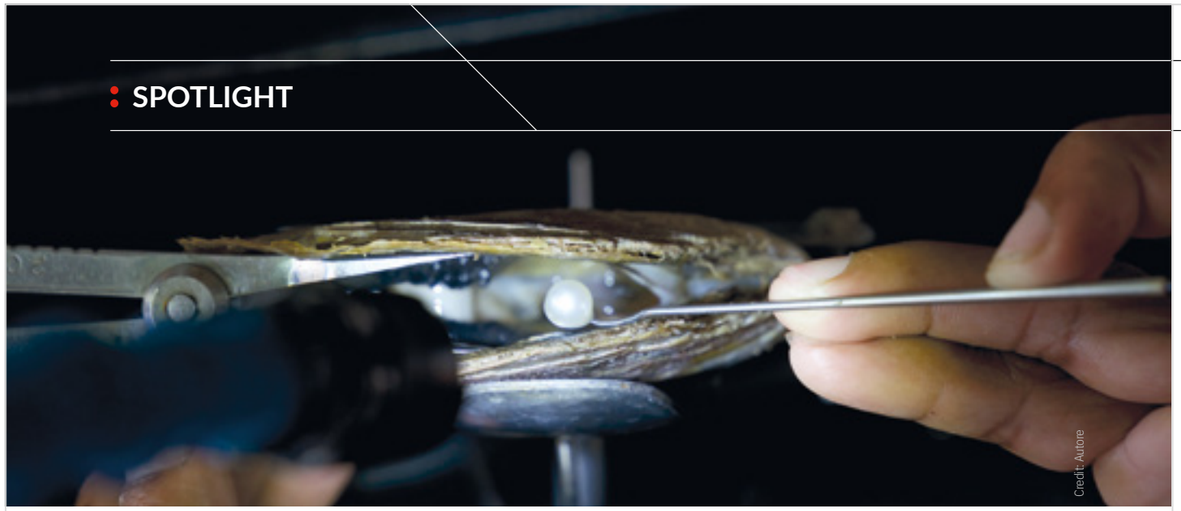
Menu Specialties

- ***Lamb tagine*** – it is a very unique dish. El Bazar has probably sold 10,000 lamb tagines throughout the five years it has been open and has never received negative feedback. Nearly everyone who eats it is amazed, and shares this feedback. It is also a family dish, and wonderful for sharing. The El Bazar staff is confident they can always deliver a quality, unique experience with this one.
- ***Seafood platter*** – most people coming to Lombok want to eat seafood. With this dish, guests can experience a wide range of different types of seafood, tasting new flavors, and being amazed by the presentation. As is a theme at El Bazar, this dish is also perfect for sharing. (Oh, and it is about half the cost that one would pay in Bali).
- ***Unique veggie options*** – vegetarians and vegans can comfortably be satisfied at El Bazar. Cauliflower green couscous and roasted eggplant with coconut tzatziki allow everyone at El Bazar, regardless of diet, to experience authentic Mediterranean flavors.

UPCOMING NEWS

- ***Venue refresh*** (spoiler alert!)
- ***Friday steaks night*** – one night a week, El Bazar will feature six types of cuts from across the world – Scotland, Australia, Japan, and the US, to name a few. Each steak can be prepared and cooked in different ways, according to the wishes of the customer. Guests can choose the steak, the cut (rib eye, rump, brisket), the sauce (béarnaise, mushroom cream, chimichurri), sides (mixed veggies, oven roasted potatoes with herbs, or roasted pumpkin). The feast will be served in a way that will awaken all the senses.
- ***More events are teed up***. Follow @elbazarlombok on Instagram or El Bazar Lombok on Facebook to learn more about what is to come.

EL BAZAR
CAFE & RESTAURANT

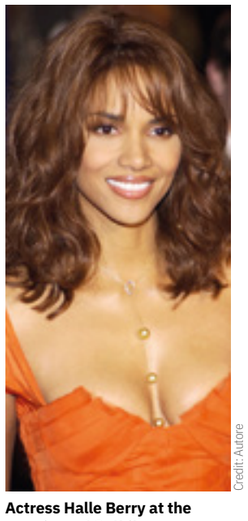


Credit: Autore

A Pearl is Born

It's a cool fall evening in late 2003. Hollywood actress Halle Berry walks the red carpet at the premiere of her new movie, Gothika, in Los Angeles, looking every bit as glamorous as the occasion, dressed in an eye-catching orange dress, matched perfectly with an elegant and unique pearl necklace.

Three years earlier, on a large, swaying boat off the coast of remote Lombok Island in Indonesia, pearl technician Adrian Sopian focuses intently on his detailed work out in the ocean. Three years, thousands of kilometers apart and seemingly polar opposite lives, yet Berry's and Sopian's worlds intersect – but how? It all starts with a five-millimeter round bead called a nucleus.



Credit: Autore

Actress Halle Berry at the premiere of Gothika.

The tiny nucleus, made from the shell of an American Pigtoe mussel from the Mississippi River, and inserted into a juvenile oyster, is what will hopefully spur the creation and growth of a perfect South Sea Pearl, at one of Autore Group's four pearl farms in the waters surrounding Lombok. But before the implantation of the nucleus into the oyster can take place, many steps have to be successfully completed. The four-year process of farmed pearls involves lots of science, planning, precision, patience – and a fair bit of Mother Nature's cooperation.

The first step in the pearl production process is to induce spawning in Autore's hatchery, by simulating the conditions for spawning in nature with small increases in water temperature, changes in salinity, increasing the pH balance, and more. The fertilized eggs hatch and turn into larvae, approximately 60 micrometers – 6 hundredths of a millimeter – in size, which are then grown and fed in the hatchery until they are ready to be moved into the ocean. That's where Iwan, farm site manager at Autore's Teluk Nara hatchery in northwest Lombok comes in. Originally from rural and largely poor Sumbawa island, to the east of Lombok, Iwan has worked in the pearl industry for 22 years, and passionately cares for the oysters he is responsible for rearing for two years. They will slowly grow from 1.5-millimeter baby oysters into 10-centimeter juvenile oysters – spats – ready for the nucleus implantation. The Teluk Nara location has been carefully selected for its tidal movement, water temperature, salinity and nutritional availability – perfectly suited for baby oysters to grow. As the farm site manager, Iwan carefully monitors the daily conditions of the growing oysters, adjusting the duties for each supervisor at each pontoon at each site in the ocean depending on the conditions of the day. After Iwan and his staff have reared, cleaned and nurtured the oysters for two years, the spats are ready to be implanted with the nucleus and start growing pearls.

AUTORE AT A GLANCE

- Autore was founded in Australia in 1991.
- In Lombok, the company employs 500-600 local employees, and four foreigners.
- The Autore Group is one of the largest South Sea Pearl companies in the world.
- In addition to its four Lombok sites, Autore also has three locations in Sumbawa and one in Jawa.

> Any given day, Autore normally has 600,000 oysters with pearls growing in them and another 600,000 juveniles waiting for the implant in the water.

One of Autore's pearl farms.

Credit: Autore

In Sekotong, in southwest Lombok, Adrian Sopian leans in with intense concentration, his body counteracting the rolling motion of the boat his workstation is located on. With a small instrument in his steady hand, he carefully inserts the nucleus into the juvenile oyster shell that's ever so slightly opened, with the goal of one day being able to harvest a beautiful south sea pearl from that oyster. But Adrian will

Credit: Best in Lombok

Cleaning and repairing the nets is time-consuming work.

Credit: Best in Lombok

Pearl technician Adrian Sopian at his implantation work station.

Credit: Autore

Autore pearl farm.

Gifts From Lombok

The best memories are those created through experiences, but bringing home a few mementos is also part of travelling, whether keeping them for ourselves, or sharing them with our nearest and dearest. **Lombok is a haven for unique and local handicrafts, with many villages specialising in one particular craft.**

If you fancy a day trip to handicraft villages, head to Sukarara, Sade and Pringgasela for traditional weaving; Banyumulek, Masbagik and Penujak for pottery; Labuapi and Rungkang Jangkuk for wooden masks and carvings; and Beleka and Kotaraja for rattan handicrafts.

For one-stop-shopping, so-called oleh-oleh shops sell a collection of souvenirs and crafts, from batik clothes to sarongs, woven baskets, Lombok foods and everything in-between. You can find numerous large oleh-oleh shops in Senggigi, Mataram and Praya, and a couple of smaller ones in Kuta.

Be prepared to bargain or negotiate prices if you don't see a price tag. This is normal, and expected.

1 Pearl bracelet, Autore 2 Traditional wooden mask 3 Beach sarongs 4 Rattan purse 5 Textile & wood necklace, Lombalio 6 Braided pandan leaf bag 7 Lava rock & stone bracelets 8 Traditional wooden statue 9 Painted wooden bowls 10 Braided decorative platter

Q/A Practical Tips

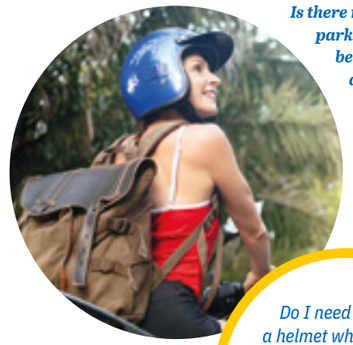
Can I use credit cards in Lombok?
The majority of hotels, restaurants and shopping malls accept credit cards (+3% bank fee), however, it is always advisable to carry enough cash for the day, since most smaller shops, warungs, surf schools, vehicle rentals and transport operators do not accept cards. You'll find many ATMs throughout Lombok, at bank offices (e.g. BNI, BCA, Mandiri), convenience stores, as well as inside some hotels (e.g. Novotel). The maximum withdrawal amount might be lower than you are used to.

Where can I stock up on food?
Most convenience stores sell basic foods, such as yogurt, milk, cereals, noodle cups, coffee and juices. In Kuta, Fresh Market; Banyu Urip and Tri Putri, as well as local fruit and vegetable stands along the main roads, sell the basics for cooking meals at home. In Senggigi, Temptations; CocoMart and Fresh Market also sell basic staples. **Bread & pastry delivery: NICO Boulangerie T/WA: +62 (0)819 9922 1166**

Can I purchase a local phone card with Internet access?
Yes, you can buy local phone cards at many locations throughout Lombok, at the airport, convenience stores and local shops. Be prepared to show your passport when you purchase your SIM card.

Do I need an international driver's license to rent a scooter, motorbike or car?
Legally you are required to have an international driver's license to drive any vehicle in Indonesia. You need to carry the international license and your original license when driving. You can obtain an international driver's license while in Lombok, but it can be a time-consuming process. You most likely will not be asked to show a valid international license when you rent a vehicle, but your travel insurance will not cover you if you have an accident while driving without a valid international license.

What is the cost to rent a scooter or car?
On average, the price for a scooter rental is 50,000 Rp per day, and a car without a driver 300,000 Rp per day.



Is there normally a parking fee near beaches or other destinations?
Yes, there is a parking fee almost everywhere. Ask to receive a parking receipt (tiket), and keep it on your person until you have picked up your vehicle. This is your proof that you have paid, in case something happens to your vehicle. It is advised you pay the fee and park in the parking area. If you choose not to pay and park elsewhere outside the parking area, there is a chance your vehicle could get damaged or stolen. Along beaches, the

Do I need to wear a helmet when driving a scooter or motorbike?
Yes, all drivers of scooters and motorbikes are required by law to wear a helmet.

Don't get caught with a 1,000,000 Rp per day overstay fee!

Know which type of visa you have, and whether it's extendable. Visa extensions must be done in person at Immigration in Mataram a minimum of 7 days before expiration.

1. Free 30-day visa on arrival (non-extendable)
2. Paid 30-day visa on arrival (extendable once)
3. Multiple-entry business visa (60-day max. stay, valid for 1 year, non-extendable)
4. Single-entry business visa (valid for 60 days, extendable 4 times)
5. Social-cultural visa (valid for 60 days, extendable 4 times)

Before you go to Immigration, prepare the following paperwork, originals and a copy:

- Passport (Immigration will keep the passport during the extension process)
- The visa sticker in your passport (and the receipt, if you have it)
- Application form from Immigration
- Departure ticket to leave Indonesia

Questions about your visa or the visa extension process?
Contact DES Consultants:
dewi.ita2982@gmail.com
+62 (0)818 548 971

02. *Przetargi Publiczne* magazine

Przetargi Publiczne is a specialist monthly for lawyers and public officials, in a practical and accessible way describing issues in the field of public procurement, which both contracting entities and contractors face on a daily basis. The magazine systematically provides its readers with reliable information on the correct application of public procurement law and changes taking place in the regulations. It is made up of the most outstanding specialists in this field.

Scope of work:
– design
– layout
– typography
– desktop publishing
– pre-press

Cover by Krzysztof Kanoniak

↑ Click to move to Table of Contents

Profesjonalnie i praktycznie o zamówieniach publicznych

MIESIĘCZNIK

PRZETARGI PUBLICZNE

10
2018

nr 10 (155) październik 2018 | cena 33,00 zł (w tym 5% VAT) | www.przetargipubliczne.pl

RAPORT SPECJALNY

8

Koncepcja Nowego Prawa Zamówień Publicznych

Opublikowana w czerwcu 2018 r. „Koncepcja nowego Prawa Zamówień Publicznych" prezentuje wizję nowej ustawy, mającej zastąpić uchwaloną w 2004 r. ustawę Prawo zamówień publicznych.

ISSN 1895-0825

32 **Otwarcie ofert bez ofert**
Jak przeprowadzić czynność otwarcia ofert, gdy w postępowaniu nie wpłynęła żadna ważna oferta?

42 **Instytucja przystąpienia**
W treści przystąpienia przystępujący musi wykazać interes w uzyskaniu rozstrzygnięcia na korzyść strony, do której przystępuje.

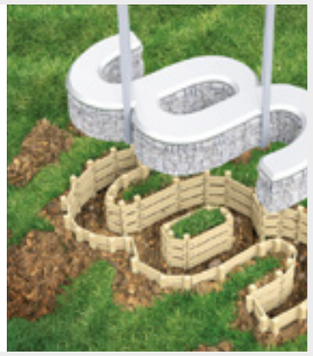
KSIĄŻKA GRATIS
„Przetarg nieograniczony w procedurze odwróconej – aspekty praktyczne"

SPIS TREŚCI

TEMAT NUMERU

Koncepcja nowego pzp

Jakie propozycje zmian – szczególnie w zakresie procedury uproszczonej, umów w sprawie zamówień i środków odwoławczych – przewidziano w dokumencie prezentującym koncepcję nowego prawa zamówień publicznych? – **s. 8**



PRZETARGI PUBLICZNE

ADRES REDAKCJI
ul. Krakowska 29, 50-424 Wrocław
tel. 71 797 28 46
faks 71 797 28 16

ADRES INTERNETOWY
www.przetargipubliczne.pl
redakcja@przetargipubliczne.pl

REDAKTOR NACZELNA
Elżbieta Sobczuk
elzbieta.sobczuk@przetargipubliczne.pl

SEKRETARZ REDAKCJI
Anna Mazurek
anna.mazurek@przetargipubliczne.pl

RADA PROGRAMOWA
mec. Zbigniew Pawlak – przewodniczący,
Halina Olszowska – członek honorowy,
Ewa Wiktorowska, mec. Irena Skubiszak-Kalinowska,
Iwona Ziarniak, prof. Andrzej Panasiuk,
mec. Renata Tubisz, Jacek Jerka

KOREKTA
Bogusława Otfinowska

PROJEKT GRAFICZNY I SKŁAD
Marcin Szewczyk
dtp@presscom.pl

WYDAWCA
PRESSCOM Sp. z o.o.
ul. Krakowska 29, 50-424 Wrocław
www.presscom.pl
biuro@presscom.pl

PREZES ZARZĄDU
Paweł Podkański

DYREKTOR WYDAWNICZY
Przemysław Golis

REKLAMA
Mikołaj Marzec
tel. 71 797 48 05 / tel. kom. 606 792 942
mikolaj.marzec@presscom.pl

Alina Merchelska
tel. kom. 604 174 172
alina.merchelska@presscom.pl

Patrycja Kubiak-Rogalna
tel. kom. 728 980 807
patrycja.kubiak@presscom.pl

PATRONATY
Jacek Śmieszek-Świętalski
tel. 71 797 28 30
jacek.smieszek@presscom.pl

PRENUMERATA
tel. 71 797 28 34
prenumerata@przetargipubliczne.pl
www.przetargipubliczne.pl
Santander Bank Polska S.A.
96 1090 1522 0000 0001 0162 2418

Nakład 5000 egz.

Okładka
Krzysztof Kanoniak

Wydawca jest członkiem
Izby Wydawców Prasy

Elżbieta Sobczuk
redaktor naczelna

Prace nad nowym pzp

Dziś, po bez mała 20 latach funkcjonowania systemu zamówień publicznych w Polsce, nikt nie ma już wątpliwości, że oczekiwania wobec sposobu, w jaki wydawane są środki publiczne, bardzo się zmieniły. Nie wystarczy już, by dostawy, usługi i roboty budowlane były jak najtańsze – muszą one być jeszcze wysokiej jakości, a sposób ich realizacji powinien uwzględniać najnowsze możliwości techniczne i innowacje.

Efektywne wydatkowanie środków publicznych, zakładające osiągnięcie oszczędności w sektorze publicznym przy jednoczesnym wzroście poziomu jakości nabywanych dóbr czy usług, z całą pewnością wymaga przejrzystej i spójnej regulacji prawnej o randze ustawy.

Niestety, obecnie obowiązująca ustawa Prawo zamówień publicznych (a ściślej mówiąc – zamówienia publiczne realizowane na jej podstawie) stanowi duże wyzwanie zarówno dla zamawiających, jak i dla wykonawców, dlatego obie te grupy, w szerokich konsultacjach społecznych dotyczących założeń do nowej ustawy, zgłosiły wiele postulatów, które pozwoliły na identyfikację głównych problemów dotyczących sposobu i zakresu kontraktowania dostaw, usług i robót budowlanych w systemie zamówień publicznych.

Na podstawie zdefiniowanych w ten sposób problemów określono pewne priorytety dla koncepcji nowej ustawy, którymi są m.in.: zwiększenie konkurencyjności postępowań, większa ich transparentność, większy dostęp do rynku zamówień dla MŚP, usprawnienia proceduralne (w tym wyodrębnienie procedury udzielania zamówień poniżej progów unijnych), zwiększenie roli współpracy zamawiających z wykonawcami, lepsze zarządzanie procesem zawierania oraz realizacji umowy, dostępny proces odwoławczy czy też usprawnienie systemu kontroli.

Najważniejsze założenia wspomnianej koncepcji analizujemy i oceniamy w raporcie specjalnym *Koncepcja nowego pzp*.

Nowe prawo zamówień

Jak należy ocenić propozycje zmian w systemie zamówień publicznych w Polsce, zawarte w przygotowanym przez MPiT i UZP dokumencie pt. Koncepcja nowego Prawa Zamówień Publicznych?

Ewa Wiktorowska
inżynier budownictwa, prezes zarządu OSKZP, członek Rady KIG, doradca, były trener z listy Prezesa UZP i arbiter

Koncepcję nowego Prawa Zamówień Publicznych **i zawarte w niej propozycje zmian w systemie zamówień publicznych w Polsce oceniam bardzo pozytywnie**. Proponowane modyfikacje w zakresie uporządkowania przepisów dotyczących udzielania zamówień wskazują na prawidłową diagnozę stanu, w jakim obecnie znajduje się ten system, i na właściwie wytyczone cele. Planowane rozwiązania – zwłaszcza te dotyczące: polityki zakupowej państwa, zwiększenia efektywności zamówień, ochrony wykonawców z rynku MŚP, systemu środków ochrony prawnej, a także położenie większego nacisku na realizację umowy w sprawie zamówienia publicznego i na poprawę kontroli – uważam za bardzo potrzebne.

Uważam, że szczególnie podkreślić trzeba bardzo dobrą propozycję ułatwienia etapu badania ofert i potwierdzania przez wykonawców zdolności do wykonania zamówienia i braku podstaw wykluczenia. Obejmuje ona dwa nowe, nieznane jeszcze w Polsce instrumenty, takie jak integracja rejestrów i certyfikacja przez jednostkę publiczną. Popieram wprowadzenie procedury uproszczonej w zamówieniach o wartościach poniżej progów UE i zmniejszenie ilości wyłączeń ze stosowania przepisów pzp.

Aby jednak osiągnąć zamierzony w Koncepcji cel, konieczne jest opracowanie przykładowych wzorów dokumentów przetargowych. Zauważyć też należy, że wielość procedur może utrudniać wykonawcom z rynku MŚP dostęp do zamówień. Zgadzam się z potrzebą właściwego podziału ryzyk w umowie i zwiększenia równowagi stron umowy, z ewaluacją realizacji tej umowy, z zapisami dotyczącymi płatności częściowych i zaliczek, a także z koncepcją wprowadzenia do pzp klauzul abuzywnych.

Pamiętajmy jednak, że dopiero zapoznanie się z konkretnymi przepisami pozwoli na ocenę, czy przyjęte kierunki zmian zostaną osiągnięte.

Jacek Jerka
prawnik, dyrektor departamentu zakupów w NBP, członek zarządu OSKZP; praktyk i doradca, szkoleniowiec i wykładowca

W *Koncepcji nowego Prawa Zamówień Publicznych* wyraźnie podkreślono znaczenie zamówień publicznych dla wspierania rozwoju gospodarczego, innowacyjności, realizowania polityk społecznych, strategii państwa oraz poprawy jakości nabywanych dóbr i usług, a także dla wspierania firm z sektora MŚP. Zmiany, które w tym kontekście zasygnalizowano w Koncepcji, a które należy zaaprobować, to:

1) profesjonalizacja osób po stronie zamawiającego;
2) wzmocnienie roli Prezesa UZP jako wspierającego zamawiającego w prawidłowym przeprowadzaniu postępowań;
3) sporządzanie analizy poprzedzającej wszczęcie postępowań „o dużych wartościach";
4) wprowadzenie „wstępnych konsultacji rynkowych" oraz umożliwienie zorganizowania spotkania informacyjnego z wykonawcami na etapie przygotowania postępowania;
5) wyraźne wyodrębnienie możliwości dokonania opisu przedmiotu zamówienia za pomocą opisu funkcjonalnego;
6) wprowadzenie zasady efektywności, jako jednej z podstawowych zasad zamówień;
7) zastrzeganie zamówień dla wykonawców z sektora MŚP lub dla zatrudniających osoby defaworyzowane;
8) utrzymanie warunków i przesłanek wykluczenia w zakresie aspektów społecznych czy środowiskowych;
9) uproszczenie postępowań krajowych;
10) wprowadzenie klauzul abuzywnych w umowach i obligatoryjnej waloryzacji umów;
11) zapewnienie zaskarżalności postanowień umownych, a także innych czynności i zaniechań w postępowaniach krajowych.

Wdrożenie proponowanych zmian będzie „obciążać" zamawiających, UZP czy KIO, co wymaga odpowiedniego uwzględnienia w skutkach regulacji.

W PRAWIE

Od 4 września 2018 r. obowiązują przepisy ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o zwalczaniu nieuczciwej konkurencji oraz niektórych innych ustaw (DzU z 2018 r., poz. 1637).

5 września 2018 r. zaczęła obowiązywać ustawa z dnia 20 lipca 2018 r. o zmianie ustawy o odpadach oraz niektórych innych ustaw (DzU z 2018 r., poz. 1592).

Od 11 września 2018 r. obowiązuje rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. zmieniające rozporządzenie w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (DzU z 2018 r., poz. 1750).

11 września 2018 r. weszła w życie ustawa z dnia 5 lipca 2018 r. o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (DzU z 2018 r., poz. 1544).

19 września 2018 r. wiążące stały się przepisy ustawy z dnia 5 lipca 2018 r. o zmianie ustawy o partnerstwie publiczno-prywatnym oraz niektórych innych ustaw (DzU z 2018 r., poz. 1693).

19 września 2018 r. ogłoszono tekst rozporządzenia Rady Ministrów z dnia 11 września 2018 r. w sprawie wysokości minimalnego wynagrodzenia za pracę oraz wysokości minimalnej stawki godzinowej w 2019 r. (DzU z 2018 r., poz. 1794).

Wytyczne MIiR w zakresie przygotowania projektów PPP

W ramach realizacji polityki rządu w zakresie rozwoju partnerstwa publiczno-prywatnego, przyjętej przez Radę Ministrów w lipcu 2017 r., Ministerstwo Inwestycji i Rozwoju opracowało wytyczne dotyczące przygotowania projektów PPP. Wytyczne są zbiorem praktycznych rekomendacji dotyczących tego, jak krok po kroku przygotować niezbędne analizy, aby decyzja o wszczęciu postępowania na wybór partnera prywatnego w trybie zamówienia publicznego lub procedury koncesyjnej była właściwa.

Wytyczne w zakresie przygotowania projektów PPP są pierwszą z trzech publikacji na temat realizacji projektów PPP. Kolejne części Wytycznych będą obejmować opis procedury związanej z postępowaniem dotyczącym wyboru partnera prywatnego oraz wzory umów PPP i koncesji ze stosownymi komentarzami. Tom pierwszy Wytycznych wraz z załącznikami dostępny jest na stronie **www.ppp.gov.pl**.

Wsparcie dla zamawiających

Urząd Zamówień Publicznych udostępnił nową opinię prawną, która dotyczy zamówień na usługi społeczne i inne szczególne usługi o wartości równej lub przekraczającej progi z art. 138g pzp, a także opublikował kolejne przykładowe dokumenty: regulamin postępowania o udzielenie zamówienia publicznego na usługi społeczne i inne szczególne usługi, o których mowa w art. 138g ust. 1 pzp; wzór umowy o świadczenie usług prawnych. Z treścią dokumentów można zapoznać się na stronie **www.uzp.gov.pl**.

Opinia w sprawie planowanego projektu PPP

Zgodnie z art. 3b znowelizowanej ustawy o PPP każdy podmiot publiczny, który planuje realizację inwestycji w formule partnerstwa publiczno-prywatnego, może wystąpić do ministra właściwego ds. rozwoju regionalnego o uzyskanie opinii nt. zasadności realizacji przedsięwzięcia w ramach PPP (tzw. Opinia PPP). Na stronie www.ppp.gov.pl dostępna jest opracowana przez MIiR procedura uzyskania Opinii PPP.

Zmiany w wyłączeniach stosowania pzp oraz ustawy o umowie koncesji na roboty budowlane lub usługi

Od 1 października 2018 r. obowiązują zmiany w przepisach pzp oraz ustawy o umowie koncesji na roboty budowlane lub usługi, które zostały wprowadzone ustawą z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę Prawo o szkolnictwie wyższym i nauce (DzU z 2018 r., poz. 1669). Zmiana pzp polega na dodaniu do art. 4 pzp punktu 13a, który wprowadza nową przesłankę wyłączającą stosowanie pzp w odniesieniu do umów, o których mowa w art. 149 ust. 2 ustawy z dnia 3 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (art. 81 ustawy Przepisy wprowadzające ustawę Prawo o szkolnictwie wyższym i nauce), czyli w zakresie powierzenia spółce celowej, w drodze umowy:

- zarządzania prawami do wyników działalności naukowej lub do know-how związanego z tymi wynikami w zakresie komercjalizacji bezpośredniej;
- zarządzania infrastrukturą badawczą.

W ustawie o umowie koncesji na roboty budowlane lub usługi zmieniony został natomiast art. 5 ust. 1 pkt 2 lit. e odnoszący się do przesłanki wyłączenia stosowania tej ustawy do umów koncesji w dziedzinach obronności i bezpieczeństwa (art. 155 ustawy Przepisy wprowadzające ustawę Prawo o szkolnictwie wyższym i nauce). Zmiana brzmienia ww. przepisu wynika z potrzeby dostosowania do pojęcia „badania naukowe" wprowadzonego ustawą Prawo o szkolnictwie wyższym i nauce, do którego do tej pory na gruncie ustawy o umowie koncesji odnoszono się przez określenia: „podstawowe badania" i „badania stosowane".

Źródło: www.uzp.gov.pl

Nowe drogi rowerowe w Koninie

22 września 2018 r. w Koninie oddano do użytku ponad 8 kilometrów nowych dróg rowerowych. Ścieżki i ciągi pieszo-rowerowe zrealizowano w ramach inwestycji „Stworzenie zintegrowanego systemu komunikacji publicznej na terenie KOSI". Projektem zostało objęte miasto Konin oraz gminy: Golina, Kazimierz Biskupi, Kramsk, Krzymów, Rzgów, Stare Miasto, Ślesi n, które wspólnie tworzą Koniński Obszar Strategicznej Interwencji (KOSI). W ramach projektu powstało także 8 punktów przesiadkowych i 11 wypożyczalni rowerów miejskich.

Tczewskie tereny rekreacyjne

Niecka Czyżykowska, Bulwar Nadwiślański, ul. Flisaków – te trzy tereny rekreacyjne zostaną dofinansowane z budżetu państwa w ramach programu „Narodowe dziedzictwo tczewskich terenów nad Wisłą przywracamy społeczeństwu miasta". 17 września 2018 r. prezydent Tczewa Mirosław Pobłocki oraz wojewoda pomorski Dariusz Drelich podpisali umowę na dofinansowanie nadwiślańskich inwestycji kwotą blisko 1,6 mln zł. Prezydent Tczewa wierzy, że kolejne inwestycje nad Wisłą sprawią, iż miasto stanie się bogatsze w infrastrukturę do wypoczynku i rekreacji, służącą wszystkim mieszkańcom. Dotacja wykorzystana zostanie jeszcze w tym roku. Pieniądze zostaną oficjalnie włączone do budżetu miasta korektą budżetową podczas najbliższej sesji Rady Miejskiej.

Parkingi w Poznaniu

Spółka Poznańskie Inwestycje Miejskie ogłosiła przetarg na projekt, budowę i wyposażenie trzech parkingów typu Park&Ride w Poznaniu. Projekt obejmuje budowę nowych utwardzonych nawierzchni placów i zatok parkingowych o łącznej pojemności minimum 207 stanowisk postojowych. Oferty można było składać do 9 października.
Do zadań wykonawcy w każdej lokalizacji będą należały m.in.: prace rozbiórkowe i przygotowawcze, przygotowanie infrastruktury podziemnej, ułożenie nawierzchni, wykonanie ogrodzenia, montaż oświetlenia i monitoringu wizyjnego, kas biletowych oraz terminali wjazdowych i wyjazdowych, automatycznych sanitariatów, małej architektury oraz tablic informacyjnych. W każdym przypadku wykonawca będzie miał maksymalnie 410 dni na zakończenie realizacji zadania.

Prawo do przedsiębiorczości

W ramach projektu „Prawo do przedsiębiorczości", mającego na celu wsparcie przedsiębiorców z sektora MŚP, we wrześniu i październiku organizowane są spotkania na terenie całej Polski, podczas których mikro, mali i średni przedsiębiorcy mogą pozyskać wiedzę o nowych rozwiązaniach, w tym dotyczących zamówień publicznych, które ułatwiają prowadzenie działalności gospodarczej w Polsce. W projekcie tym aktywnie uczestniczy Urząd Zamówień Publicznych, a działania podejmowane przez UZP z myślą o przedsiębiorcach są ukierunkowane na odformalizowanie postępowań i ułatwienia proceduralne. Celem tych działań jest zwiększenie udziału sektora MŚP w rynku zamówień publicznych oraz podniesienie poziomu zainteresowania przetargami wśród tych przedsiębiorców. Więcej informacji na prawodoprzedsiebiorczosci.parp.gov.pl.

Rys. Bartłomiej Brosz

50
to liczba ogłoszeń o konkursie, zamieszczonych od początku br. w Biuletynie Zamówień Publicznych (stan na 1 września 2018 r.).

222
tyle ogłoszeń o zmianie umowy zostało opublikowanych na stronach TED od początku roku 2018.

26
w sumie tyle ogłoszeń związanych z udzielaniem koncesji pojawiło się na stronach BZP i TED od początku tego roku.

9%
tylko tyle postępowań ogłaszanych w krajowym publikatorze przewidywało cenę jako jedyne kryterium oceny ofert.

99,43%
tyle postępowań w procedurze krajowej wszczęto w trybie przetargu nieograniczonego.

JACHRANKA, 15–17 października 2018 r.

XIII Forum Przetargów Publicznych – relacja

W organizowanej już po raz trzynasty najważniejszej w Polsce konferencji poświęconej zamówieniom publicznym uczestniczyło rekordowo liczne grono osób, które na co dzień zajmują się tą tematyką – zarówno od strony zamawiających, jak i wykonawców.

Fot. Marcin Oliva-Soto

Tegoroczna edycja odbyła się pod hasłem przewodnim „Prawo zamówień publicznych w kontekście problemów występujących w praktyce i orzecznictwie, z uwzględnieniem rodo i elektronizacji". Aspekt elektronizacji zamówień publicznych i nowych zasad ochrony danych osobowych towarzyszył wykładom i warsztatom prowadzonym w toku całej konferencji.

Najważniejszym celem wydarzenia było pogłębienie i ugruntowanie wiedzy na temat stosowania prawa zamówień publicznych oraz wymiana doświadczeń nabywanych podczas prowadzenia postępowań o udzielenie zamówień publicznych i uczestniczenia w nich. Wystąpienia, które miały miejsce podczas Forum, zostały przygotowane przez uznanych ekspertów i praktyków. Opierając się na konkretnych przykładach, starali się oni odpowiedzieć na najpilniejsze pytania i wątpliwości uczestników systemu zamówień w Polsce.

Patronaty XIII Forum Przetargów Publicznych

- Urząd Zamówień Publicznych
- Ogólnopolskie Stowarzyszenie Konsultantów Zamówień Publicznych
- Związek Gmin Wiejskich Rzeczypospolitej Polskiej

Wystąpienia Gości Specjalnych

Koncepcja nowego Prawa Zamówień Publicznych

W ramach swojego wystąpienia pierwszy z naszych Gości Specjalnych, pan Hubert Nowak (p.o. Prezesa Urzędu Zamówień Publicznych, Wiceprezes UZP) wspomniał o dwóch dużych przedsięwzięciach prowadzonych równolegle przez UZP:

- przygotowanie projektu nowego prawa zamówień publicznych – przedsięwzięcie jest prowadzone wraz z Ministerstwem Przedsiębiorczości i Technologii, a zostało zainicjowane ponad 2 lata temu;
- elektronizacja zamówień publicznych.

Te dwa przedsięwzięcia mocno na siebie wpływają i są ze sobą ściśle powiązane.

W ramach pierwszego z nich powstała *Koncepcja nowego Prawa Zamówień Publicznych*. Jak wskazał Pan Prezes, koncepcja ta – która docelowo ma zostać przekuta w nowe prawo zamówień – nie pogodzi wszystkich zgłoszonych uwag i wniosków, jakie otrzymano od uczestników systemu zamówień w Polsce, będzie ona musiała wyważyć różne interesy, różnorodność perspektyw, pluralizm poglądów na temat problemów związanych ze stosowaniem procedur prawa zamówień, tak aby nowe regulacje – wypracowane w perspektywie 25 lat funkcjonowania systemu – były dobre i użyteczne.

Koncepcja ma 2 cele strategiczne:

- stworzenie warunków do realizacji polityki zakupowej państwa (w synergii z postulatami Strategii na rzecz Odpowiedzialnego Rozwoju z lutego 2017);
- zapewnienie efektywnego wydatkowania środków publicznych.

Dodatkowym celem jest uregulowanie aspektów, które funkcjonują od 2 lat (po nowelizacji z 2016 r.), a dotąd były pozostawione doktrynie i orzecznictwu.

Cele szczegółowe to m.in.: zwiększenie konkurencyjności, zwiększenie dostępności do zamówień dla MŚP, nacisk na lepsze zaplanowanie i przygotowanie zamówienia i jego wykonania (zdrowo-rozsądkowość), zwiększenie współpracy między zamawiającym a wykonawcą, większa transparentność postępowania, usprawnienie systemu kontroli, identyfikacja zamówień strategicznych (wymagających zastosowania innych reżimów), dopracowanie zagadnień związanych z zamówieniami zielonymi, zrównoważonymi i innowacyjnymi.

Prace legislacyjne nad nowym pzp

Nasz drugi Gość Specjalny, pani dr Joanna Knapińska (Zastępca Dyrektora Departamentu Doskonalenia Regulacji Gospodarczych w Ministerstwie Przedsiębiorczości i Technologii) przedstawiła harmonogram prac legislacyjnych nad nowym pzp, wskazując, że część tych prac już została zrealizowana, a mianowicie:

- wskazanie – w ramach Strategii na rzecz Odpowiedzialnego Rozwoju – na potrzebę zwiększenia efektywności zamówień publicznych (luty 2017);
- przeprowadzenie cyklu debat z uczestnikami rynku zamówień publicznych (luty 2017);

Goście Specjalni: Joanna Knapińska i Hubert Nowak

Goście Specjalni: Małgorzata Stręciwilk, Janusz Niedziela, Małgorzata Rakowska, Jerzy Pieróg

- powołanie zespołu odpowiedzialnego za przygotowanie koncepcji nowego pzp (sierpień 2017);
- przeprowadzenie kilkudziesięciu spotkań i konsultacji na temat problemów w systemie zamówień publicznych (II połowa 2017 r.);
- przygotowanie *Koncepcji nowego Prawa Zamówień Publicznych* (maj 2018 r.), a następnie zorganizowanie spotkań w różnych miastach i przeprowadzenie ankiety dotyczącej zagadnień poruszonych w Koncepcji (wskutek tych działań otrzymano kilkadziesiąt stanowisk pisemnych).

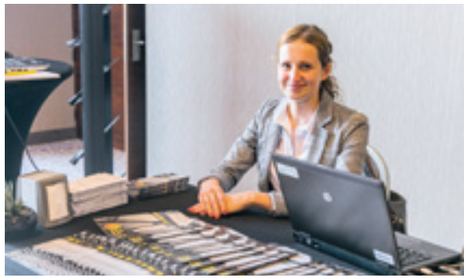
Obecnie trwają prace nad nowym pzp, w ścisłej współpracy między UZP i MPiT. Zgodnie z planem w listopadzie projekt ustawy ma być gotowy do wysłania do konsultacji publicznych i międzyresortowych, tak by w marcu projekt ten mógł być przyjęty przez Radę Ministrów. Zakładanym terminem uchwalenia nowej ustawy przez parlament jest czerwiec lub wrzesień 2019 r. z *vacatio legis* wyznaczonym na 1 stycznia 2020 r.

Pani Dyrektor podkreśliła, że liczba uwag i wniosków dotyczących stosowania pzp, jakie wpłynęły do Ministerstwa i UZP od uczestników systemu zamówień publicznych, przerosła najśmielsze oczekiwania. Wskazała, że zespół pracujący nad tekstem nowej ustawy stara się pochylić nad każdym przesłanym wnioskiem, mając przy tym świadomość, że nie da się pogodzić wszystkich. Jednak celem prac zespołu jest stworzenie przepisów przejrzystych, jasnych i precyzyjnych.

Warsztaty

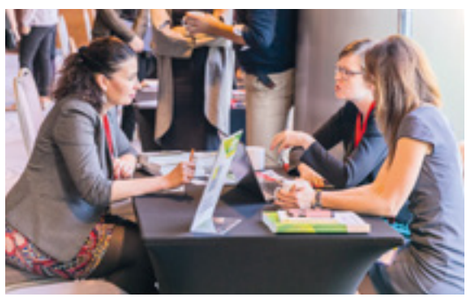
Po południu drugiego dnia Forum odbyły się zajęcia warsztatowe, podczas których uczestnicy mieli okazję wymienić się opiniami i doświadczeniami. Spotkania prowadzone były równolegle w sześciu grupach tematycznych:

- Zasady korzystania przez wykonawców z potencjału podmiotów trzecich w praktyce i orzecznictwie – **mec. Marzena Jaworska**
- Aktualność i ważność dokumentów składanych w ofertach w postępowaniu o udzielenie zamówienia publicznego w praktyce i orzecznictwie – **mec. Piotr Trębicki**
- JEDZ elektroniczny – obowiązki i uprawnienia wykonawcy – **Iwona Ziarniak**
- Zasada proporcjonalności przy formułowaniu warunków udziału wykonawców w postępowaniu o udzielenie zamówienia publicznego w praktyce i orzecznictwie – **Grzegorz Soluch**
- Procedura wyjaśniania rażąco niskiej ceny: obowiązek wszczęcia procedury, wyłączenie tego obowiązku a możliwość wszczęcia procedury, terminy na złożenie wyjaśnień i dowody w postępowaniu wyjaśniającym w praktyce i orzecznictwie – **Ewa Żak**
- Praktyczne wykorzystanie próbki w postępowaniu o udzielenie zamówienia publicznego – **Paweł Trojan**



Stanowisko Urzędu Zamówień Publicznych

Partner Strategiczny – Market Planet



Stoliki eksperckie

- Kancelaria Radców Prawnych Brudkiewicz, Suchecka i Partnerzy
- CZUBLUN TRĘBICKI Kancelaria Radców Prawnych Sp. p.
- Jaworska Matusiak Grześkowiak-Stojek Jarnicka Kancelaria Prawna Sp. j.
- Kancelaria prawna Jerzykowski i Wspólnicy Sp. k.
- PIERÓG & Partnerzy Kancelaria Prawna
- Kancelaria Prawna Schampera, Dubis, Zając i Wspólnicy Sp. k.

Kryształy Przetargów Publicznych 2018

15 października 2018 r. po raz dziesiąty rozdano Kryształy Przetargów Publicznych – nagrody dla najlepszych zamawiających i wykonawców. Uroczysta gala wręczenia nagród odbyła się w Jachrance podczas otwarcia XIII Forum Przetargów Publicznych.

Od 10 lat celem nagrody jest promocja i upowszechnianie stosowania najlepszych zasad i praktyk w dziedzinie zamówień publicznych zarówno po stronie zamawiających, jak i wykonawców. W tegorocznej edycji zgłaszane były zadania zakończone między 1 sierpnia 2017 r. a 31 lipca 2018 r. Kapituła Nagrody, spośród 100 nadesłanych zgłoszeń, wybrała 5 zwycięzców.

KATEGORIA I – zadania na rzecz ochrony środowiska lub gospodarki wodnej

- **Zamawiający: Przedsiębiorstwo Komunikacji Miejskiej Sp. z o.o. z siedzibą w Sosnowcu**

Zakup niskoemisyjnego taboru autobusowego w Przedsiębiorstwie Komunikacji Miejskiej Sp. z o.o. w Sosnowcu

KATEGORIA II – inwestycje wpływające na poprawę funkcjonowania infrastruktury drogowo-komunikacyjnej

- **Zamawiający: Gmina Miasto Kołobrzeg**

Przebudowa ścieżki rowerowej do Podczela w ramach projektu „Analiza transgranicznej turystyki rowerowej wraz z rozbudową wybranych odcinków międzynarodowej trasy rowerowej"

- **Wykonawca: SZCZĘŚNIAK Pojazdy Specjalne Sp. z o.o.**

Dostawa 26 sztuk samochodów ratownictwa technicznego (z żurawiem) dla Komendy Wojewódzkiej Państwowej Straży Pożarnej we Wrocławiu

KATEGORIA III – inwestycje z zakresu przebudowy lub budowy obiektów użyteczności publicznej lub rewitalizacji przestrzeni publicznej

- **Zamawiający: Urząd Miejski w Będzinie**

Budowa plaży miejskiej – obiektu sportowo-rekreacyjnego oraz zagospodarowanie terenów nadrzecznych Czarnej Przemszy

- **Wykonawca: Warbud SA**

Realizacja budynku Sądu Rejonowego w Nowym Sączu – zaprojektowanie, wybudowanie, sfinansowanie oraz utrzymanie nowej siedziby Sądu w formule partnerstwa publiczno-prywatnego

Na zdjęciu laureaci nagrody (od lewej): Paweł Żółtak – **Warbud SA**; Ewa Latos – **Urząd Miejski w Będzinie**; Grzegorz Szczęśniak – **SZCZĘŚNIAK Pojazdy Specjalne Sp. z o.o.**; Anna Żelazna – **Przedsiębiorstwo Komunikacji Miejskiej Sp. z o.o. z siedzibą w Sosnowcu**

Patronat honorowy

- Ministerstwo Infrastruktury
- Ministerstwo Środowiska
- Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej
- Polska Izba Inżynierów Budownictwa
- Instytut Badawczy Dróg i Mostów
- Izba Projektowania Budowlanego

Patronat medialny

- Grupa Biznes Polska
- Miesięcznik „Finanse Publiczne"

Kapituła Nagrody

- Ewa Wiktorowska – Przewodnicząca
- dr Włodzimierz Dzierżanowski
- adw. Grzegorz Mazurek
- prof. Andrzej Panasiuk
- mec. Zbigniew Pawlak
- Elżbieta Sobczuk

Serdecznie gratulujemy laureatom i dziękujemy wszystkim uczestnikom. Już dziś zapraszamy do udziału w 11. edycji nagrody Kryształy Przetargów Publicznych.

WALORYZACJA PŁATNOŚCI NA RZECZ WYKONAWCY

Okoliczności i sposoby zmiany wynagrodzenia

Zwiększenie kwoty należnej wykonawcy możliwe jest m.in. na podstawie art. 142 ust. 5 i art. 144 ust. 1 pkt 6 pzp, gdzie określono przesłanki warunkujące możliwość waloryzacji oraz jej granice.

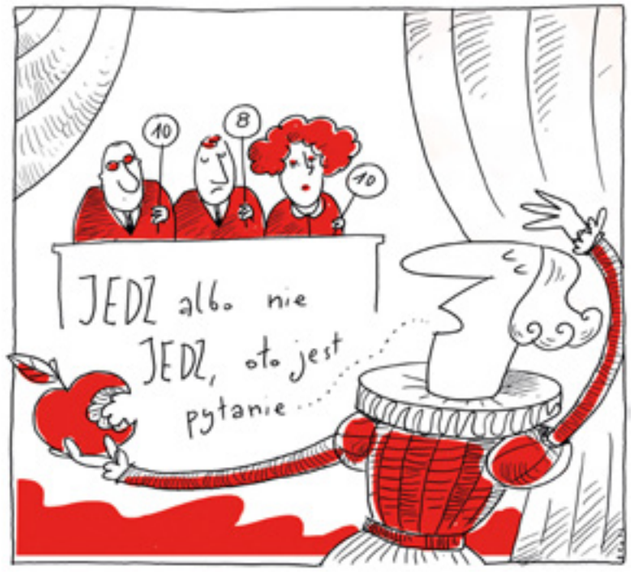
Grzegorz Mazurek
adwokat, prowadzi własną kancelarię prawną; były wiceprezes Krajowej Izby Odwoławczej i arbiter

W roku 2018 można było zaobserwować sytuacje, w których kontrakty zawarte lub planowane w wyniku upływu czasu okazywały się nierentowne, a wykonawcy próbowali podwyższyć wynagrodzenie, względnie – rezygnowali z kontraktów. Problem ten dotyczy najczęściej firm z branży budowlanej, ale nie tylko – również branża usług, w których istotnym elementem kosztu jest wynagrodzenie pracowników, charakteryzuje się tendencją do podwyższania wynagrodzeń. W obecnych realiach trudne jest utrzymanie stałych cen w kontraktach. Nie sposób przewidzieć wzrostu kosztów w okresie od wygrania przetargu do zakończenia realizacji zamówienia, a niekiedy nawet w okresie od wygrania przetargu do podpisania umowy z zamawiającym.

Jako przykład niecodziennej sytuacji, gdzie wykonawca złożył odwołanie na wybór własnej oferty, można wskazać przypadek wykonawcy Impresa Pizzarotti. W lipcu 2017 r. do oddziału GDDKiA Oddział w Białymstoku w przetargu na projekt i budowę drogi ekspresowej S61 wpłynęło 11 ofert. Budżet zamawiającego wynosił 963,554 mln zł, a ceny ofert wahały się od 442,875 mln zł do 711,707 mln zł. Najtańszą, a zarazem wybraną do realizacji ofertę złożyła firma Impresa Pizzarotti – wartość tej oferty stanowiła zaledwie 45% budżetu przewidzianego przez zamawiającego. Decyzję o wyborze właśnie tej oferty podjęto w grudniu 2017 r., lecz z powodu szeregu odwołań na wybór wykonawcy postępowanie znacznie się wydłużyło. W marcu 2018 r., tj. po 8 miesiącach od terminu złożenia ofert, zamawiający ponownie dokonał wyboru oferty wykonawcy Impresa Pizzarotti. Tym razem od wyboru najkorzystniejszej oferty odwołał się wybrany wykonawca. Postępowanie Impresa Pizzarotti najprawdopodobniej związane było ze zmianą kosztów realizacji inwestycji. Należy wskazać, że w lipcu 2017 r. zarówno koszty pracy,

Motyw 109 preambuły do dyrektywy 2014/24/UE

Instytucje zamawiające mogą napotkać okoliczności zewnętrzne, których nie mogły przewidzieć w momencie udzielania zamówienia, w szczególności gdy zamówienie jest wykonywane przez dłuższy czas. W takim przypadku niezbędny jest pewien stopień elastyczności w celu dostosowania umowy do tych okoliczności bez konieczności przeprowadzania nowego postępowania o udzielenie zamówienia. Pojęcie niemożliwych do przewidzenia okoliczności odnosi się do okoliczności, których nie można było przewidzieć pomimo odpowiednio starannego przygotowania pierwotnego postępowania o udzielenie zamówienia przez instytucję zamawiającą, z uwzględnieniem dostępnych jej środków, charakteru i cech tego konkretnego projektu, dobrych praktyk w danej dziedzinie oraz konieczności zagwarantowania odpowiedniej relacji pomiędzy zasobami wykorzystanymi na przygotowanie postępowania a jego przewidywalną wartością (...).



Rys. Bartłomiej Brosz

przepis art. 22 pzp stosuje się odpowiednio);

- art. 116 ust. 2 pkt 6 (regulamin konkursu określa w szczególności informację o oświadczeniach lub dokumentach, jakie mają dostarczyć uczestnicy konkursu w celu potwierdzenia spełnienia stawianych im wymagań, przepis art. 25 pzp stosuje się odpowiednio);
- art. 118 ust. 3 pzp (uczestnicy konkursu mogą wspólnie brać udział w konkursie; przepisy dotyczące uczestnika konkursu stosuje się odpowiednio do uczestników konkursu biorących wspólnie udział w konkursie);
- art. 120 ust. 3 pzp (do oceny wniosków o dopuszczenie do udziału w konkursie przepisy art. 26 ust. 3 i 4 pzp stosuje się odpowiednio);
- art. 122 ust. 1 pzp (sąd konkursowy ocenia prace konkursowe zgodnie z kryteriami określonymi w ogłoszeniu o konkursie; przepis art. 87 ust. 1 pzp stosuje się odpowiednio);
- art. 124 pzp (zamawiający unieważnia konkurs, jeżeli nie został złożony żaden wniosek o dopuszczenie do udziału w konkursie lub żadna praca konkursowa, a w przypadku, o którym mowa w art. 111 ust. 1 pkt 2, co najmniej dwie prace konkursowe, albo jeżeli nie rozstrzygnięto konkursu; do unieważnienia konkursu przepisy art. 93 ust. 1 pkt 6 i 7 pzp stosuje się odpowiednio).

W związku z licznymi wątpliwościami dotyczącymi treści regulaminu konkursu w zakresie wymagań stawianych uczestnikom warto zwrócić szczególną uwagę na sposób formułowania i weryfikacji wymagań podmiotowych i odpowiedniego zastosowania przepisów dotyczących kwalifikacji uczestników konkursu do etapu składania prac konkursowych.

Konkurs nie stanowi trybu udzielenia zamówienia, może natomiast poprzedzać przeprowadzenie postępowania i stanowić etap przygotowania do realizacji określonego zamierzenia inwestycyjnego.

Formułowanie i weryfikacja wymagań podmiotowych oraz kwalifikacja uczestników konkursu

Zgodnie z art. 120 ust. 1 pzp zamawiający dopuszcza do udziału w konkursie i zaprasza do składania prac konkursowych uczestników konkursu spełniających wymagania określone w regulaminie konkursu. Wymagania, o których tu mowa, nie mają swojej definicji legalnej. Sam przepis nie odnosi się do warunków udziału w postępowaniu i podstaw wykluczenia określonych w art. 22 i 24 pzp. Dopiero w sytuacji gdy organizator przewidzi w konkursie nagrody w postaci zaproszenia do negocjacji bez ogłoszenia co najmniej dwóch autorów wybranych prac konkursowych lub zaproszenie do negocjacji w trybie zamówienia z wolnej ręki autora wybranej pracy konkursowej, art. 22 pzp należy stosować odpowiednio.

W tym wypadku przepis stanowi niejako wstępne przygotowanie organizatora i samych uczestników konkursu do udziału w postępowaniu o udzielenie zamówienia publicznego w jednym ze wskazanych trybów. Zabieg ten jest o tyle istotny, że podstawy wykluczenia będą już obligatoryjnie weryfikowane przez zamawiającego podczas postępowania w trybie negocjacji bez ogłoszenia lub w trybie z wolnej ręki. W postępowaniach tych mogą mieć zastosowanie również warunki udziału, czyli zamawiający może zechcieć sprawdzić np. doświadczenie lub uprawnienia architektów (zweryfikować zdolności techniczne lub zawodowe wykonawcy). Stąd też w konkursach, w których przewidziano

OŚWIADCZENIE WOLI WYKONAWCY

Pojęcie oferty

W systemie zamówień publicznych pojęcie oferty ma niebagatelne znaczenie. Zależy od niego bowiem kształt decyzji podejmowanych przez zamawiającego i wykonawców, w tym kwestia podstawowa: czy oferta złożona przez wykonawcę odpowiada treści siwz.

Mariusz Partyka
prawnik specjalizujący się w tematyce zamówień publicznych

W myśl art. 14 pzp do czynności podejmowanych przez zamawiającego i wykonawców w postępowaniu o udzielenie zamówienia stosuje się przepisy ustawy Kodeks cywilny (dalej: kc), jeżeli przepisy ustawy nie stanowią inaczej. Omawiając kwestie związane z pojęciem oferty, trzeba się odwołać do przepisów kc, gdyż w tym przypadku mamy do czynienia z taką właśnie sytuacją – pzp nie zawiera bowiem definicji tego pojęcia.

Oferta w rozumieniu ustawy Kodeks cywilny

Wypracowany i utrwalony przez orzecznictwo sposób rozumienia oferty opiera się na regulacji art. 66 § 1 kc. Powołując się na ugruntowane już orzecznictwo, KIO podkreśla, że oferta, jako jeden z rodzajów oświadczenia woli prowadzących do zawarcia umowy, powinna zawierać istotne postanowienia umowy (zob. wyroki: KIO 721/09, KIO 24/10, KIO 945/15 i KIO 236/17; a także KIO 1463/17, KIO 1381/17, KIO 1397/17, KIO 2475/17, KIO 18/18, KIO 476/18 i KIO 595/18). Izba zwraca uwagę, że treść oferty na gruncie pzp należy rozumieć w sposób ścisły i utożsamiać ją z oświadczeniem wykonawcy, z którego wynika zobowiązanie względem zamawiającego w związku z realizacją przyszłej umowy (zob. wyrok KIO z 14 maja 2009 r., KIO 570/09). O zakresie zobowiązania wyrażonego w ofercie wykonawcy w pierwszej kolejności przesądza jego treść, której materialnym substratem jest pismo wykonawcy przedstawiające np. w formie formularza ofertowego cenę, sposób wykonania czy inne warunki zobowiązania, które wykonawca podejmuje (zob. wyrok KIO z 26 czerwca 2009 r., KIO 721/09).

Wymagania w stosunku do zobowiązania zamawiający określa w siwz. Oprócz wymagań kształtujących zakres zobowiązania wykonawcy w siwz ujmowane są również postanowienia formalne, jak np. dotyczące sposobu przedstawienia oferty, czy informacyjne, jak informacja o miejscu otwarcia ofert, czy też postanowienia o charakterze ubocznym. Jako przykład postanowień ubocznych można podać oświadczenie w zakresie rodo czy oświadczenie dotyczące tego, czy wykonawca należy do MŚP.

> Niedopuszczalne jest prowadzenie między zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty oraz, z zastrzeżeniem poprawienia innej omyłki, dokonywanie jakiejkolwiek zmiany w jej treści.

W wyroku z 13 kwietnia 2018 r. (KIO 588/18) Izba dokonała podziału na warstwę merytoryczną i formalną oferty, podkreślając, że każdy wymóg postawiony przez zamawiającego w siwz co do formy składanych ofert może być traktowany wyłącznie jako zalecenie sporządzenia oferty we wskazany sposób, nie zaś jako bezwzględny obowiązek wykonawców (zob. też orzecznictwo sądowe, np. wyrok Sądu Okręgowego w Gdańsku z 8 maja 2013 r., XII Ga 186/13). Podobnie w wyroku z 21 sierpnia 2017 r. (KIO 2155/16), gdzie do kwestii formalnych Izba zaliczyła takie wymagania, jak sposób sporządzenia i przedstawienia oferty, w tym: wygląd i liczba formularzy (ale nie treść zawartych w nich oświadczeń), numeracja stron, spis treści itp.

Izba wielokrotnie wskazywała na to, co składa się na zakres pojęciowy oferty, podając na bazie określonych stanów faktycznych poszczególnych odwołań również konkretne przykłady.

odrębnie udzielane wymagają zastosowania różnych przepisów pzp.

Proces planowania zamówień publicznych jest działaniem dynamicznym. Zatem istnieje możliwość wystąpienia w ciągu roku budżetowego nieprzewidzianych, wcześniej niezaplanowanych zamówień. W takiej sytuacji wartość zamówienia, którego potrzeba ujawniła się po lub w trakcie udzielania zaplanowanego wcześniej zamówienia tego samego rodzaju, nie podlega sumowaniu z wartością innych, już udzielonych lub udzielanych zamówień. W przypadku tego typu zamówień zamawiający powinni stosować procedury odpowiednie do ich wartości. Istotne jest, aby zamawiający umiał wykazać i uzasadnić brak możliwości przewidzenia danego zamówienia na etapie tworzenia planu oraz udowodnić, że dochował należytej staranności na etapie planowania.

Przedstawione w planie dane, w szczególności wartość zamówienia, nie są wiążące dla zamawiającego przez cały rok. Wartość zamówienia, którą zamawiający podaje w planie, jest wartością przybliżoną (orientacyjną). W związku z tym jeżeli w ciągu roku budżetowego wystąpią zmiany w planie finansowym, to zamawiający powinien dokonać uaktualnienia planu zamówień. Zamawiający w treści planu powinni unikać niedookreślonych pojęć typu „rezerwa" czy „usługi pozostałe".

Zawartość planu postępowań

W art. 13a ust. 2 pzp jednoznacznie wskazuje się, że zamawiający powinien określić w planie postępowań:
1) przedmiot zamówienia;
2) rodzaj zamówienia według podziału na zamówienia na roboty budowlane, dostawy lub usługi;
3) przewidywany tryb lub inną procedurę udzielenia zamówienia;
4) orientacyjną wartość zamówienia;
5) przewidywany termin wszczęcia postępowania w ujęciu kwartalnym lub miesięcznym.

Plan postępowań o udzielenie zamówień

Zgodnie z art. 13a ust. 1 pzp zamawiający, o których mowa w art. 3 ust. 1 pkt 1 i 2, oraz ich związki, nie później niż 30 dni od dnia przyjęcia budżetu lub planu finansowego przez uprawniony organ, sporządzają plany postępowań o udzielenie zamówień, jakie przewidują przeprowadzić w danym roku finansowym, oraz zamieszczają je na stronie internetowej. W analizowanym przepisie ustawodawca posługuje się pojęciem „postępowania o udzielenie zamówień". Zgodnie z przyjętą w art. 2 pkt 7a pzp definicją przez postępowanie o udzielenie zamówienia rozumie się postępowanie wszczynane w drodze publicznego ogłoszenia o zamówieniu lub przesłania zaproszenia do składania ofert albo przesłania zaproszenia do negocjacji w celu dokonania wyboru oferty wykonawcy, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, lub – w przypadku trybu zamówienia z wolnej ręki – wynegocjowania postanowień takiej umowy. W związku z tym publikacja omawianych planów dotyczy wyłącznie zamówień, do których zamawiający mają obowiązek stosować przepisy pzp. Zatem zamówień, do których przepisy pzp nie mają zastosowania (w szczególności zamówień do 30 000 euro), nie ujmuje się w planie postępowań o udzielenie zamówienia publicznego, chyba że są one udzielane na podstawie art. 6a pzp i stanowią część zamówienia[1].

Zakres podmiotowy

Obowiązek sporządzania planu postępowań spoczywa na zamawiających, o których mowa w art. 3 ust. 1 pkt 1 i 2 pzp, oraz ich związkach.

Zamawiający – zobowiązani do stosowania pzp – inni niż wskazani wprost w art. 13a ust. 1 pzp, nie mają obowiązku sporządzania planu postępowań, lecz biorąc pod uwagę dobre praktyki rynkowe, jak również podejście organów kontroli do przygotowania i przeprowadzenia postępowań o udzielenie zamówienia publicznego, warto także im rekomendować sporządzenie takiego planu i zamieszczenie go na własnej stronie internetowej.

Wymienione w ustawie elementy planu stanowią katalog otwarty (co wynika z zastosowanego w przepisie sformułowania „w szczególności"). Zatem zamawiający mogą opublikować również dodatkowe dane dotyczące poszczególnych planowanych postępowań, które w ich ocenie powinny się w tym planie znaleźć. W planie postępowań należy uwzględnić postępowania wszczynane w danym roku, których realizacja jest przewidziana

Korzyści z opracowania planu zamówień publicznych

Prawidłowo sporządzony plan zamówień publicznych w szczególności:
1) umożliwi terminowe przygotowanie, przeprowadzenie, udzielenie i zrealizowanie zamówienia;
2) pozwoli uniknąć łączenia zamówień, które odrębnie udzielane wymagają zastosowania różnych przepisów pzp;
3) pozwoli uniknąć dzielenia zamówienia na części;
4) ułatwi zamawiającemu udzielanie zamówienia w częściach, w szczególności na podstawie art. 6a pzp;
5) umożliwi podjęcie prawidłowej decyzji w przypadku wystąpienia konieczności udzielenia zamówienia niezaplanowanego lub awaryjnego;
6) pozwoli na osiągnięcie zysku (redukcji kosztów);
7) pozwoli na efektywne zarządzanie potencjałem kadrowy oraz stanami magazynowymi.

Grzegorz Mazurek
adwokat, prowadzi własną kancelarię prawną; były wiceprezes Krajowej Izby Odwoławczej i arbiter

o udzielenie zamówienia publicznego na wykonywanie usług teletransmisji oraz usług dostępu do internetu. Przedmiot zamówienia został podzielony na 149 części. Częścią zamówienia zgodnie z siwz było świadczenie usługi w danej lokalizacji, przy czym w odniesieniu do niektórych lokalizacji zamawiający przewidział zamówienie dwóch usług dla jednej lokalizacji, a każda z tych usług stanowiła odrębną część zamówienia (np. Urząd Dzielnicy Ochota – części 7 i 8). Jest to o tyle istotne, że z takim podziałem zamówienia korespondowały określone zasady odpowiedzialności wykonawców z tytułu kar umownych za nienależyte wykonanie usług wyrażone we wzorze umowy załączonym do siwz. Zamawiający przewidział kary umowne m.in. z tytułu awarii usługi, jednak ekspozycja na te kary oraz sama wysokość kar uzależnione zostały od tego, czy dany wykonawca dostarcza jedną czy dwie usługi do danej lokalizacji. Dla przykładu – w przypadku wystąpienia jednej awarii usługi w danym miesiącu, jeżeli wykonawca dostarczałby tylko jedną usługę w danej lokalizacji, w ogóle nie byłby zobowiązany do zapłaty kary umownej, natomiast jeżeli wykonawca dostarczałby dwie usługi w danej lokalizacji, to nawet pojedyncza awaria skutkowałaby naliczeniem temu wykonawcy kary w wysokości 50% miesięcznego wynagrodzenia. W przypadku wystąpienia czterech awarii w danym miesiącu wykonawcy dostarczającemu tylko jedną usługę w danej lokalizacji naliczona zostałaby kara umowna w wysokości 75% miesięcznego wynagrodzenia, natomiast wykonawcy świadczącemu dwie usługi w tej lokalizacji – w wysokości 300% miesięcznego wynagrodzenia. Zatem wykonywanie dwóch części zamówienia w danej lokalizacji (czyli złożenie ofert na obie części) przez jednego wykonawcę bardzo istotnie zwiększało ryzyko odpowiedzialności z tytułu kar umownych, jak i samą wysokość tych kar.

Odwołującym był wykonawca, który złożył oferty na wiele części, w tym również w tych lokalizacjach, w których istniał podział na dwie części – tam w każdym przypadku złożył oferty na obie części.

Wśród wykonawców konkurujących z odwołującym było dwóch wykonawców należących do tej samej grupy kapitałowej, którzy złożyli oferty w taki sposób, że ofertę na jedną z części dla danej lokalizacji złożył jeden z tych wykonawców, na drugą zaś – drugi.

Zamawiający wyodrębnił 27 lokalizacji, dla których zamawiane były dwie odrębne usługi (łącznie zatem 54 części zamówienia). W odniesieniu do 26 takich lokalizacji ofertę na jedną z usług złożyła jedna spółka, a na drugą – druga spółka z tej samej grupy kapitałowej. Druga spółka złożyła ofertę w takim zakresie, aby była ona komplementarna względem oferty pierwszej spółki, tj. obejmowała wyłącznie drugą z usług, jaka miała być świadczona w danej lokalizacji. Zdaniem odwołującego dowodzi to, że wykonawcy zawarli porozumienie mające na celu zakłócenie konkurencji i że osiągnęli korzyść względem pozostałych oferentów. Gdyby bowiem ofertę na wykonanie zamówienia złożył wyłącznie jeden z tych wykonawców, obejmując jej zakresem wszystkie części zamówienia, to wówczas znacząco wzrosłoby ryzyko ekspozycji tego wykonawcy na odpowiedzialność z tytułu kar umownych, jak i na wysokość tych kar. Złożenie oferty przez każdego z tych wykonawców należących do tej samej grupy kapitałowej w opisany powyżej sposób pozwoliło im na uniknięcie obowiązku zapłaty istotnie wyższej lub zwielokrotnionej kary umownej.

Wykonawcy złożyli oświadczenia o przynależności do jednej grupy kapitałowej, potwierdzając fakt istnienia powiązań

Zachwiana konkurencja

Zgadzam się, że możliwość zakłócenia konkurencji przy składaniu ofert częściowych nastąpi w sytuacji, gdy zamawiający ograniczył możliwość składania ofert do np. dwóch części, a dwie firmy z jednej grupy kapitałowej, w uzgodnieniu, składają ofertę na większą liczbę części – tj. jedna z nich na dwie i druga na dwie. W tym zakresie mogę odnieść się do orzeczeń Krajowej Izby Odwoławczej: wyroku z 6 marca 2017 r. (KIO 283/17, KIO 291/17, KIO 298/17) i wyroku z 12 października 2017 r. (KIO 2053/17, KIO 2054/17), w których wskazano na konieczność wykluczenia wykonawcy w takiej sytuacji.
Natomiast nie zgadzam się z twierdzeniem o zachwianiu konkurencji w przypadku składania ofert na różne części przez spółki z tej samej grupy kapitałowej, gdy zamawiający nie ograniczył możliwości składania ofert do określonej liczby części. Warunkiem jest tutaj, aby części tego zamówienia nie były powiązane w taki sposób, że tworzą współzależność, która rzutowałaby na różną sytuację wykonawców. W takim przypadku możliwość zachwiania konkurencji jest wyłącznie teoretyczna i nieodczuwalna dla wykonawców.

Rodzaje środków zaradczych

Zdiagnozowanie istnienia realnej szansy wzięcia udziału w postępowaniu o udzielenie zamówienia przez podmiot uczestniczący w jego przygotowaniu aktualizuje po stronie zamawiającego obowiązek wdrożenia rozwiązań mających na celu zapobieżenie zakłóceniu konkurencji. Zastosowane przez zamawiającego środki powinny w szczególności być skuteczne oraz proporcjonalne.

Z uwagi na:

1) przykładowy katalog środków, jakie ustawodawca zaproponował zamawiającemu do zastosowania (tj. przekazanie pozostałym wykonawcom informacji, które uzyskał i przekazał podczas przygotowania postępowania, oraz wyznaczenie odpowiedniego terminu na składanie ofert);
2) wyraźne zakazanie naruszania zasady ochrony konkurencji, w tym przy kreowaniu dokumentacji postępowania o udzielenie zamówienia z naruszeniem zasady otwarcia na konkurencję (zob. art. 29 ust. 2 pzp; art. 31a ust. 2 pzp);
3) możliwość skorzystania przez wykonawców ze środków ochrony prawnej na sporządzenie opisu przedmiotu zamówienia z naruszeniem wymogu ochrony uczciwej konkurencji, w tym również w przypadku tzw. zamówień o wartości krajowej (art. 180 ust. 2 pkt 5 pzp)

– zasadne wydaje się przyjęcie, że środki zastosowane przez zamawiającego powinny przede wszystkim służyć wyrównaniu pozycji podmiotów ubiegających się – lub mogących się ubiegać – o udzielenie zamówienia przez zagwarantowanie im uzyskania takiego samego zakresu wiedzy o zamówieniu, takiego samego czasu na sporządzenie oferty itp.

Zasadniczo będą to zatem środki wskazane przykładowo w art. 31d pzp.

Obowiązek informacyjny

Zamawiający oprócz konieczności zastosowania odpowiednich środków w celu przywrócenia równowagi między wykonawcami zobowiązany jest również do wskazania w protokole, jakie środki zostały przez niego podjęte (art. 31d pzp). Tożsamy obowiązek sprawozdawczy ciąży na zamawiającym, jeżeli to wykonawca wykazuje, że jego udział w postępowaniu zapewnia niezakłócenie konkurencji (art. 24 ust. 10 pzp). Spełnienie obowiązku informacyjnego ma szczególnie istotne znaczenie ze względu na umożliwienie zweryfikowania przez podmioty trzecie, w tym wykonawców, zasadności bądź niezasadności niewyeliminowania wykonawcy, który uprzednio brał udział w przygotowaniu postępowania. Nałożony na zamawiającego obowiązek informacyjny, który należy spełnić przy sporządzaniu protokołu z postępowania (w przypadku druku ZP-PN, część 3 pkt 2), jest w praktyce również cennym przypomnieniem o konieczności zdiagnozowania niezbędności wdrożenia środków zaradczych na podstawie art. 31d pzp.

Nie jest jednak wykluczone zastosowanie przez zamawiającego środków innych niż wymienione w art. 31d pzp, a nadto nienakazanych do zastosowania mocą innych przepisów pzp – np. wykreowanie opisu przedmiotu zamówienia w sposób nieograniczający konkurencji (zob. wyrok KIO z 19 października 2018 r., KIO 2037/18).

Przerzucenie obowiązku na wykonawcę

Spełnienie przez zamawiającego omawianego obowiązku ma niezwykle istotne znaczenie również ze względu na obowiązujące regulacje dotyczące wykluczenia wykonawcy z postępowania. Mocą art. 24 ust. 10 pzp, jeżeli zamawiający nie zastosował środków usuwających lub niwelujących zakłócenie konkurencji, ciężar podjęcia odpowiednich działań spoczywa na wykonawcy. W myśl art. 24 ust. 10 pzp wykonawca, przed wykluczeniem go z postępowania na podstawie art. 24 ust. 1 pkt 19 pzp, ma możliwość udowodnienia, że jego udział w przygotowaniu postępowania nie zakłóci konkurencji. Jak zauważa KIO w wyroku z 25 października 2018 r. (KIO 1974/18), wykonawca ma mniejsze możliwości niż zamawiający w tym zakresie, a nadto nałożono na niego obowiązek udowodnienia podjęcia takich działań lub, co istotne, udowodnienia, że jego udział nie zakłóci konkurencji (a więc że istnieją obiektywne czynniki za tym przemawiające). Niedogodność sprostania obowiązkowi dowodowemu potęgowana jest okolicznością, że – zgodnie ze stanowiskiem KIO – udział wykonawcy w przygotowaniu postępowania jest przez ustawodawcę traktowany każdorazowo jako zakłócenie konkurencji:

> **Wyrok KIO z 25 października 2018 r. (KIO 1974/18)**
> „Oznacza to, że (...) mamy w tym przypadku do czynienia z funkcjonowaniem pewnego rodzaju domniemania, które zakłada, że każdy taki udział jest zakłóceniem konkurencji – niezależnie od jego wymiaru, zakresu, formy, czy też rodzaju. W ogóle ustawodawca nie wypowiada się w tym zakresie ograniczając konstrukcję hipotezy tej normy do samego faktu «udziału w przygotowaniu postępowania o udzielenie zamówienia» dwukrotnie używając tego zwrotu w przepisie art. 24 ust. 1 pkt 19 ustawy Pzp. Udział

Stan elektronizacji

Proces elektronizacji zamówień publicznych jest już w toku. W najbliższym czasie sposób składania elektronicznej oferty czy JEDZ będzie się dynamicznie zmieniać: **1 października 2018 r. ma zostać uruchomiony miniPortal**, funkcjonujący do czasu wdrożenia modelu docelowego, jakim będzie Platforma e-Zamówień.

e-ZAMAWIAJĄCY

Magdalena Michałowska

Tabela 1. Forma składania ofert w zaleleżności od wartości postępowań

Niższe od progów unijnych	Równe progom unijnym lub wyższe	
Wszczęte przed **1.01.2020 r.**	Wszczęte przed **18.10.2018 r.**	Wszczęte od **18.10.2018 r.**
Oferta w formie pisemnej (opatrzona własnoręcznym podpisem)	• Oferta w formie pisemnej (opatrzona własnoręcznym podpisem) • JEDZ w formie elektronicznej (opatrzony kwalifikowanym podpisem elektronicznym)	• Oferta w formie elektronicznej (opatrzona kwalifikowanym podpisem elektronicznym) • JEDZ w formie elektronicznej (opatrzony kwalifikowanym podpisem elektronicznym)

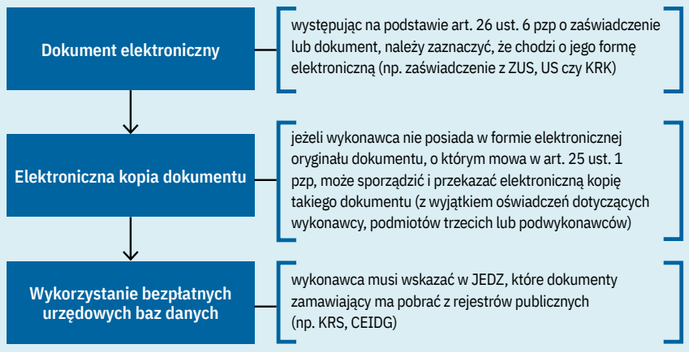
W postępowaniach wszczętych od 18 października 2018 r. zamawiający otrzymają w postaci elektronicznej (opatrzonej kwalifikowanym podpisem elektronicznym) nie tylko JEDZ, ale również oferty i wnioski o dopuszczenie do udziału w postępowaniu. Każda inna forma skutkować będzie nieważnością. Co istotne, zmiany dotyczyć będą tylko postępowań o wartościach równych kwotom wskazanym w art. 11 ust. 8 pzp lub wyższych. Nowelizacja z 20 lipca 2018 r. (DzU z 2018 r., poz. 1603) przesuwa bowiem obowiązek elektronizacji zamówień o wartości poniżej progów unijnych, prowadzonych przez innych zamawiających niż centralny zamawiający, na dzień 1 stycznia 2020 r. (zob. **tabela 1)**.

Wspomniana nowelizacja wprowadziła m.in. także zmiany w art. 2 pkt 17 w zakresie definicji środków komunikacji elektronicznej – wykreślono z niej słowo „faks" i tym samym zrównano ją z definicją zawartą w art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Ponadto w znowelizowanym art. 10a ust. 5 pzp doprecyzowano, które oświadczenia bezwzględnie muszą zostać opatrzone kwalifikowanym podpisem elektronicznym.

Oczywiście w procedurach, w których komunikacja będzie odbywała się z wykorzystaniem środków komunikacji elektronicznej, zamawiający coraz częściej będą otrzymywali elektroniczne dokumenty. Dotyczyć to będzie wszystkich dokumentów, zarówno tych przygotowywanych bezpośrednio przez wykonawcę, jak i dokumentów czy zaświadczeń urzędowych.

Pod względem technicznym sposób składania elektronicznej oferty czy JEDZ będzie się zmieniać.

Schemat. Formy dokumentów składanych w postępowaniu



1 października 2018 r. ma zostać uruchomiony miniPortal, z którego będzie można nieodpłatnie korzystać do czasu wdrożenia modelu docelowego, jakim będzie Platforma e-Zamówień.

e-WYKONAWCA

Iwona Ziarniak

Wykonawca ubiegający się o udzielenie zamówień publicznych, jako profesjonalny uczestnik systemu zamówień publicznych, musi na bieżąco śledzić zmiany, jakie zachodzą w tym systemie. Rewolucja związana z elektronizacją zamówień publicznych, która miała zawładnąć wszystkimi postępowaniami wszczętymi od 18 października 2018 r., została aktualnie podzielona na etapy, wskutek uchwalenia ustawy z dnia 20 lipca 2018 r. zmieniającej ustawę Prawo zamówień publicznych oraz ustawę o zmianie ustawy Prawo zamówień publicznych oraz niektórych innych ustaw, DzU z 2018 r., poz. 1603). Zgodnie z obecnie obowiązującymi ustaleniami termin wejścia obowiązku komunikacji zamawiającego z wykonawcą wyłącznie za pomocą środków komunikacji elektronicznej to:

– 1 stycznia 2020 r. – w przypadku zamówień, których wartość jest niższa od progów unijnych;
– 18 października 2018 r. – w przypadku zamówień, których wartość jest równa progom unijnym lub je przekracza.

Tabela 2. Stan elektronizacji – komunikacja zamawiającego z wykonawcą

Czynność	Obowiązująca forma komunikacji w zależności od wartości zamówienia	
	Zamówienia o wartości niższej od progów unijnych	Zamówienia o wartości równej progom unijnym lub przekraczającej je
Forma komunikacji	zgodnie z wyborem zamawiającego za pośrednictwem operatora pocztowego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe, osobiście, za pośrednictwem posłańca, faksu lub przy użyciu środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną	przy użyciu środków komunikacji elektronicznej
Forma (postać) oferty, wniosku o dopuszczenie do udziału w postępowaniu, oświadczenia	oferty i wnioski o dopuszczenie do udziału w postępowaniu o udzielenie zamówienia publicznego oraz oświadczenie, o którym mowa w art. 25a ustawy zmienianej w art. 1, składa się, pod rygorem nieważności, w formie pisemnej, albo – za zgodą zamawiającego – w postaci elektronicznej, opatrzone odpowiednio własnoręcznym podpisem albo kwalifikowanym podpisem elektronicznym	w postępowaniach wszczętych po 18 października 2018 r. ma zastosowanie art. 10 ust. 5 pzp, zgodnie z którym oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 25a, w tym JEDZ, sporządza się, pod rygorem nieważności, w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym
Składanie wniosku o dopuszczenie do udziału w postępowaniu lub oferty	osobiście, za pośrednictwem operatora pocztowego lub posłańca lub elektronicznie, gdy zamawiający wyraża zgodę na postać elektroniczną	w postępowaniach wszczętych po 18 października 2018 r. przy użyciu środków komunikacji elektronicznej, tj. wysłanie elektronicznej oferty lub elektronicznego wniosku za pomocą dedykowanych formularzy dostępnych na platformie e-PUAP w ramach planowanej funkcjonalności miniPortalu e-Zamówień (docelowo z wykorzystaniem platformy e-Zamówienia, portalu e-Usługi)

W **tabeli 2** przedstawiono stan elektronizacji w odniesieniu do postępowań prowadzonych przez innych zamawiających niż centralny zamawiający, po wejściu w życie wspomnianej ustawy z dnia 20 lipca 2018 r.

Wykonawca, który aktualnie ubiega się o udzielenie zamówień publicznych, których wartość jest równa progom unijnym lub je przekracza, musi:

- zapoznać się z funkcjonalnościami miniPortalu e-Zamówień (udostępnionego do czasu pełnego wdrożenia modelu docelowego zakładającego istnienie centralnej Platformy e-Zamówień), tak aby skutecznie komunikować się elektroniczne z zamawiającymi i przygotować wniosek w postaci formularza elektronicznego lub elektroniczną ofertę;
- przygotować odpowiednie zaplecze techniczne (sprzęt komputerowy, oprogramowanie, dostęp do internetu);
- posiadać ważny kwalifikowany podpis elektroniczny (spełniający wymogi bezpieczeństwa określone w ustawie z o usługach zaufania oraz identyfikacji elektronicznej) dla zapewnienia ważności czynności podejmowanych.

Rewolucja związana z elektronizacją zamówień publicznych, która miała zawładnąć wszystkimi postępowaniami wszczętymi od 18 października 2018 r., została aktualnie podzielona na etapy wskutek uchwalenia ustawy nowelizującej z dnia 20 lipca 2018 r.

ZMIANY PRAWA

Nowelizacja ustawy o PPP

Partnerstwo publiczno-prywatne nie cieszyło się dotąd zbyt dużą popularnością. Czy zmiany wprowadzone ostatnią nowelizacją przepisów o PPP zachęcą inwestorów do szerszego korzystania z tej procedury?

Martyna Lubieniecka
radca prawny, praktyk w zakresie zamówień publicznych; reprezentuje zamawiających i wykonawców przed KIO

Joanna Marczewska
prawnik; posiada doświadczenie w kontroli, prowadzeniu postępowań przetargowych oraz w reprezentowaniu wykonawców i zamawiających przed KIO

Dnia 5 lipca 2018 r. uchwalono ustawę o zmianie ustawy o partnerstwie publiczno-prywatnym oraz niektórych innych ustaw. Ustawa weszła w życie 19 września, a wprowadzone nią zmiany w zakresie przepisów ustawy o partnerstwie publiczno-prywatnym (dalej: ustawa o PPP) należy ocenić pozytywnie, mając jednocześnie nadzieję, że spowodują one większe zainteresowanie partnerstwem publiczno-prywatnym (dalej również: PPP). Znamienne jest, że podmioty publiczne w latach 2009–2017 zrealizowały jedynie 116 projektów PPP. W kontekście spodziewanego zmniejszenia finansowania unijnego wydaje się, że partnerstwo stanowi dobrą alternatywę dla realizacji zadań publicznych. Skąd więc tak znikome zainteresowanie tą formą realizacji inwestycji?

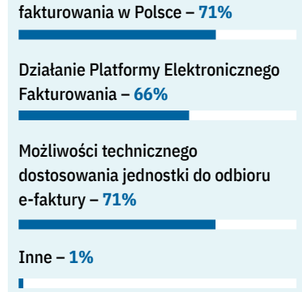
Praktyka pokazuje, że w pierwszej kolejności inwestorzy sięgają do tradycyjnych źródeł finansowania, jak dotacje, środki z funduszy UE, kredyty i pożyczki. Dopiero w ostateczności analizują możliwość zawarcia partnerstwa z podmiotem prywatnym, choć i wówczas towarzyszą temu niemałe obawy. W jednostkach samorządu terytorialnego przyczyną takiego stanu rzeczy może być brak zasobów niezbędnych do zawarcia umowy o partnerstwie, ale także braki kadrowe, brak wiedzy czy wsparcia w zakresie dokonania niezbędnych analiz i szacunków. Ponadto samorządy odczuwają obawę przed kontrolą oraz przed poniesieniem różnego rodzaju konsekwencji w obliczu ewentualnego niepowodzenia. Już sam fakt, że realizacja zamierzenia w ramach PPP oznacza współpracę z podmiotem prywatnym, wydaje się w pewien sposób zniechęcać samorządy do tej formuły. Wśród samorządowców panuje ponadto mylne mniemanie, że to podmiot prywatny powinien być obciążany wszelkim ryzykiem związanym z realizacją inwestycji, co stoi w sprzeczności z ideą partnerstwa publiczno-prywatnego, gdyż partnerstwo oparte jest na współpracy i optymalnym podziale ryzyk.

Tego rodzaju obawy powodowały, że partnerstwo nie cieszyło się zbyt dużą popularnością, stąd ustawodawca postanowił wprowadzić zmiany, które *de facto* mają doprowadzić do szerszego stosowania PPP. Z uzasadnienia

Artykuł 3a ustawy o PPP
Przed wszczęciem postępowania w sprawie wyboru partnera prywatnego podmiot publiczny sporządza ocenę efektywności realizacji przedsięwzięcia w ramach partnerstwa publiczno-prywatnego w porównaniu do efektywności jego realizacji w inny sposób, w szczególności przy wykorzystaniu wyłącznie środków publicznych.

Niezależnie od oceny własnej podmiot publiczny może wystąpić do ministra właściwego ds. rozwoju regionalnego z wnioskiem o opinię na temat zasadności realizacji przedsięwzięcia w ramach PPP.

Schemat. Obszary zainteresowań respondentów na temat e-fakturowania*



Na podstawie badania „Stan e-fakturowania w administracji publicznej. Edycja 1", E. Dobrzeniecka, W. Nogala, P. Nowak, ILiM, Poznań 2018.

Nie są fakturami elektronicznymi tzw. obrazy faktur, czyli pliki jpg, png, gif, tif czy pdf, ponieważ nie można ich automatycznie przekazać między systemami wystawcy i zamawiającego, a następnie automatycznie przetworzyć.

i ich elektronicznym odpowiednikom. Zapisy o istotności e-fakturowania uwzględnione zostały także w „Europejskiej agendzie cyfrowej" (jako jeden z siedmiu projektów przewodnich Komisji Europejskiej), w „Akcie o jednolitym rynku II" (podstawowe działanie nr 10), w „Strategii na rzecz e-zamówień" oraz komunikacie pn. „Kompleksowe e-zamówienia jako środek modernizacji administracji publicznej". Wszystkie te dokumenty wskazywały fakturowanie elektroniczne jako kluczowy element tworzenia i rozwoju jednolitego rynku cyfrowego UE[2], który znacząco przyczyni się do wzrostu gospodarczego, zwiększenia efektywności państw wspólnotowych oraz interoperacyjności i konkurencyjności działań, w szczególności w relacjach transgranicznych.

Sztandarowym dokumentem UE, wprowadzającym obowiązek odbioru faktur elektronicznych w procesach obsługi dostaw publicznych, jest dyrektywa Parlamentu Europejskiego i Rady 2014/55/UE z dnia 16 kwietnia 2014 r. w sprawie fakturowania elektronicznego w zamówieniach publicznych (DzUrz UE L 133 z 6.05.2014). Zapisy dyrektywy stosuje się do faktur elektronicznych odbieranych przez jednostki publiczne oraz wystawianych w związku z realizacją zamówień publicznych. Ważne jest, że wytyczne dyrektywy dotyczą:

- tylko faktur do zakupów i dostaw objętych dyrektywami o zamówieniach publicznych;
- tylko faktur wystawianych do jednostek sektora zamówień publicznych;
- wszystkich szczebli administracji publicznej (krajowej, regionalnej i lokalnej) w każdym kraju członkowskim UE.

Dyrektywa 2014/55/UE stwierdza, że fakturą elektroniczną jest dokument, który wykonawca wystawia i przesyła w ustrukturyzowanym formacie elektronicznym, dzięki czemu zamawiający może ją automatycznie odebrać i przetworzyć. Zatem fakturami elektronicznymi kategorycznie nie są tzw. obrazy faktur, czyli pliki jpg, png, gif, tif czy pdf, ponieważ nie można ich automatycznie przekazać między systemami wystawcy i zamawiającego, a następnie automatycznie przetworzyć. Dodatkowo e-faktura musi być zgodna z normą europejską fakturowania elektronicznego ogłoszoną decyzją wykonawczą Komisji (UE) 2017/1870 (DzUrz UE L 266 z 17.10.2017). Norma ta wskazuje obowiązujące dwa formaty, zgodnie z którymi należy przesyłać e-faktury do zamawiających w zamówieniach publicznych: UN/CEFACT i UBL 2.1. Zatem każda faktura elektroniczna, którą wykonawca wystawi i prześle w jednym z dwóch powyższych formatów, będzie musiała być odebrana i przetworzona przez podmiot zamawiający w zamówieniach publicznych na terenie UE po wejściu w życie dyrektywy 2014/55/UE.

Korzyści z wdrożenia elektronicznych faktur

- oszczędności finansowe oraz wzrost efektywności wewnętrznych i zewnętrznych procesów gospodarczych w sferze publicznej oraz u jej dostawców,
- obniżenie kosztów funkcjonowania przedsiębiorstw i wzrost ich konkurencyjności na rynku krajowym i międzynarodowym,
- obniżenie kosztów transakcyjnych w obrocie gospodarczym i w sprzedaży konsumentom indywidualnym,
- optymalizacja zarządzania płynnością firmy (np. krótsze terminy oczekiwania na płatność, minimalizacja ryzyka nadpłat bądź podwójnych płatności),
- poprawa jakości i bezpieczeństwa danych finansowych podmiotów publicznych i prywatnych,
- wzrost konkurencyjności polskiej gospodarki, w tym zwiększenie udziału polskich przedsiębiorców w rynkach zamówień publicznych innych państw członkowskich Unii Europejskiej,
- korzystny wpływ na rozwój krajowego rynku płatności bezgotówkowych,
- praktyczne stosowanie zasad zrównoważonego rozwoju – m.in. troska o środowisko naturalne przez dążenie do redukcji ilości wykorzystywanego papieru.

śmierci takiego wykonawcy roszczenia odszkodowawcze z tytułu niewykonania lub nienależytego wykonania tego rodzaju umów, powstałe przed otwarciem spadku. Na mocy art. 922 § 2 kc przedmiotem dziedziczenia nie są bowiem jedynie prawa lub obowiązki składające się na treść umowy. Z kolei powstające w następstwie niewykonania lub nienależytego wykonania zobowiązania roszczenia i obowiązki odszkodowawcze (zarówno służące wykonawcy w stosunku do zamawiającego, jak i zamawiającemu w stosunku do wykonawcy) nie są już ściśle związane z osobą spadkodawcy, co oznacza, że wejdą w skład spadku na mocy zasady generalnej płynącej z art. 922 § 1 kc.

Dziedziczenie umów w zamówieniach publicznych

Tak w przepisach kc, jak i pzp brak jest regulacji bezpośrednio dotyczącej dziedziczenia umów w sprawach zamówień publicznych. Jakkolwiek dyrektywa 2014/24/UE oraz dyrektywa 2014/25/UE po raz pierwszy w historii prawa wspólnotowego wprowadziły regulacje dotyczące zmian umów w sprawach zamówień publicznych, w tym także zmian podmiotowych, to jednak nie uregulowano w nich bezpośrednio zagadnienia sukcesji umowy w sprawie zamówienia publicznego w następstwie spadkobrania po osobie fizycznej. Do prawa polskiego unijne przepisy regulujące zmiany podmiotowe umowy zostały transponowane przez postanowienia art. 144 ust. 1 pkt 4 pzp, które również pominęły zagadnienia dziedziczenia. Do tego czasu prawo polskie nie normowało zmian podmiotowych, a poprzedni art. 144 ust. 1 pzp – w brzmieniu obowiązującym do czasu wejścia w życie nowelizacji z 22 czerwca 2016 r.[4] – regulował wyłącznie zmiany odnoszące się do przedmiotu świadczeń wynikających z umowy w sprawie zamówienia publicznego. Regulacja dyrektyw z 2014 r. oraz nowe brzmienie art. 144 ust. 1 pzp stanowią bez wątpliwości krok milowy, wychodząc naprzeciw potrzebom obrotu prawnego, jakkolwiek (w warstwie literalnej swoich postanowień) konsekwentnie milczą na temat zmiany podmiotowej umowy w sprawie zamówienia publicznego następującej wskutek spadkobrania. Mimo niedostatków regulacyjnych prawa, tak prawa wspólnotowego, jak i polskiego, należy uznać, że zarówno przepisy dyrektyw 2014/24/UE i 2014/25/UE, jak i art. 144 ust. 1 pkt 4 pzp dostarczają ważkich argumentów wskazujących kierunek wykładni art. 922 § 1 kc w zakresie, w jakim prawa i obowiązki zmarłego obejmują prawa i obowiązki wynikające z umowy w sprawie zamówienia publicznego.

Artykuł 144 ust. 1 pkt 4 lit. b pzp ewidentnie wskazuje na konieczność dokonania czynności prawnej (zmiany zawartej umowy) i wprowadza dodatkowe wymogi prawne, jakimi są spełnienie przez nowego wykonawcę warunków udziału w postępowaniu oraz niepodleganie przez niego przesłankom wykluczenia z postępowania.

Sukcesja generalna a umowa w sprawie zamówienia

Spośród wskazanych w art. 144 ust. 1 pkt 4 pzp jednostek redakcyjnych dla omawianego zagadnienia następstwa prawnego po zmarłym wykonawcy zasadnicze znaczenie ma lit. b, gdzie unormowano zmianę podmiotową umowy w sprawie zamówienia publicznego w wyniku połączenia, podziału, przekształcenia, upadłości, restrukturyzacji

Stan niepewności

Mimo zasady z art. 922 § 1 kc śmierć wykonawcy powoduje powstanie stanu niepewności co do osoby następcy prawnego. Kontrahenci zmarłego (a zatem również i zamawiający) nie wiedzą bowiem, na kogo przejdą prawa i obowiązki po zmarłym. Powołanie do spadku wynika z ustawy albo z testamentu (art. 926 § 1 kc), a krąg spadkobierców i tytuł powołania do spadku może być nieznany osobom trzecim. Dodatkowo, stosownie do treści art. 9811 § 1 kc, w testamencie sporządzonym w formie aktu notarialnego spadkodawca może postanowić, że oznaczona osoba nabywa przedmiot zapisu z chwilą otwarcia spadku (zapis windykacyjny). Przedmiotem zapisu windykacyjnego może być m.in. przedsiębiorstwo (art. 9811 § 2 pkt 3 kc). Uchylenie stanu niepewności co osoby spadkobiercy następuje w drodze aktu publicznego. Względem osoby trzeciej, która nie rości sobie praw do spadku z tytułu dziedziczenia, spadkobierca może udowodnić swoje prawa wynikające z dziedziczenia tylko stwierdzeniem nabycia spadku albo zarejestrowanym aktem poświadczenia dziedziczenia (art. 1027 kc). Jedynie w taki sposób następca prawny zmarłego wykonawcy może udowodnić zamawiającemu przejście na niego praw i obowiązków wynikających z umowy w sprawie zamówienia publicznego.

Udostępnianie załączników do protokołu postępowania

Sylwia Mosur-Blezel

Zgodnie z art. 96 pzp protokół jest jawny i sporządzany jest w trakcie prowadzenia postępowania. Oznacza to, że protokół odzwierciedla zdarzenia zaistniałe w toku postępowania, a informacja o tych zdarzeniach powinna być umieszczana w protokole niezwłocznie po ich zaistnieniu.

Załącznikami do protokołu są w szczególności: oferty, opinie biegłych, oświadczenia, zawiadomienia, wnioski, inne dokumenty i informacje składane przez zamawiającego i wykonawców oraz umowa w sprawie zamówienia publicznego. Ustawa jednoznacznie wskazuje termin udostępnienia załączników do protokołu: po dokonaniu wyboru najkorzystniejszej oferty lub unieważnieniu postępowania. Wyjątek stanowią oferty, które są udostępniane od chwili ich otwarcia. Przyjrzyjmy się orzecznictwu Krajowej Izby Odwoławczej – pozornie banalna kwestia udostępnienia protokołu postępowania i załączników do niego bywa bowiem przedmiotem odwołań wykonawców:

Wyrok KIO z 1 września 2017 r. (KIO 1632/17, KIO 1662/17)

„Wszelkie załączniki do protokołu, a więc dokumenty, które nie są ofertą, Zamawiający udostępnia po dokonaniu wyboru najkorzystniejszej oferty. W niniejszym postępowaniu Zamawiający nie dokonał czynności wyboru oferty najkorzystniejszej. Tym samym zarzut w zakresie zaniechania przez Zamawiającego udostępnienia dokumentów w postaci wezwań Zamawiającego, odpowiedzi wykonawców, wyjaśnień, pism Zamawiającego zawierających uzasadnienie odrzucenia oferty, jest bezpodstawny i podlega oddaleniu. Zamawiający będzie mógł udostępnić ww. dokumenty po dokonaniu czynności wyboru oferty najkorzystniejszej. Wbrew twierdzeniu Odwołującego, wyjaśnienia nie stanowią oferty. Są odrębnym dokumentem, a w ich treści znajduje się jedynie dookreślenie tego, co znalazło się w treści oferty. Tym samym, w ocenie Izby ujawnienie treści wyjaśnień może nastąpić dopiero od chwili wyboru oferty najkorzystniejszej".

Wyrok KIO z 15 marca 2016 r. (KIO 275/16)

„(...) zgodnie z art. 96 ust. 3 ustawy Pzp, załączniki do protokołu udostępnia się po dokonaniu wyboru najkorzystniejszej oferty. Tym samym, do chwili wyboru najkorzystniejszej oferty, zamawiający – kierując się literalnym brzmieniem przywołanego wyżej przepisu – mógłby skutecznie uchylić się od udostępnienia odwołującemu załączników do protokołu w postaci skierowanych do przystępującego wezwań oraz udzielonych przez niego wyjaśnień (lub informacji, że wyjaśnienia takie zostały złożone)".

Wyrok KIO z 21 lipca 2017 r. (KIO 1368/17)

„Zamawiający bezzasadnie odmówił udostępnienia do wglądu Odwołującego wewnętrznego dokumentu, który zawiera informacje uzyskane podczas telefonicznych konsultacji (weryfikacji) przeprowadzonych przez zamawiającego z podmiotami leczniczymi wskazanymi w Tabeli nr 3 Załącznika nr 2a, pomimo tego, że dokument taki został opracowany na potrzeby postępowania (...). Przedmiotowy dokument powinien zostać udostępniony odwołującemu jako załącznik do protokołu postępowania".

Wszelkie załączniki do protokołu, a więc dokumenty, które nie są ofertą, Zamawiający udostępnia po dokonaniu wyboru najkorzystniejszej oferty.

Warto także zwrócić uwagę na precyzyjne opisywanie w protokole załączników, aby wykonawca miał pewność, że zapoznał się z całością dokumentacji opisującej dane postępowanie. Nieprecyzyjne, zbyt ogólnikowe zapisy protokołu w zakresie wskazania załączników mogą prowadzić wykonawcę do wniosku, że udostępniono mu załączniki w sposób wybiórczy albo że zamawiający zaniechał dokonania czynności, do których jest zobowiązany w określonej sytuacji (zob. wyrok KIO z 10 maja 2016 r., KIO 616/16).

Rys. Bartłomiej Brosz

03. *IT Professional* magazine

IT Professional is a monthly magazine for IT professionals, employed in business or running their own IT services companies. In contrast to the popular computer press, *IT Professional* is of an expert nature, and the topics discussed in its pages are described in a practical way. Authors – certified and experienced specialists – focus on transferring knowledge necessary in the everyday work of IT specialists, network administrators, information security administrators, department managers and IT department directors.

Scope of work:
– design
– layout
– typography
– desktop publishing
– pre-press

Cover by Katarzyna Panek

↑ Click to move to Table of Contents

Od redakcji

Artur Cieślik
redaktor naczelny

Nowe horyzonty

Kolejny krok w rozwoju technologii kosmicznych za nami. Sonda New Horizons dotarła do Plutona, jednej z planet karłowatych naszego Układu Słonecznego. Podróż trwała ponad 3462 dni, a przebyty przez sondę dystans wyniósł prawie 32 AU (jednostki astronomiczne, 1 AU = 149,6 miliona kilometrów). Pojazd został zbudowany w technologii odpornej na radiację i pozwalającej zużywać minimum energii. Na pokładzie znajduje się siedem instrumentów badawczych zasilanych z izotopowego generatora RTG (radioisotope thermoelectric generator), który na początku lotu dostarczał około 245 W mocy! Jeżeli myślimy, że nasze komputery są energooszczędne, to jest to błąd. Każdy instrument badawczy zużywa od 2 do 10 W! Procesor sterujący, na którym działa system operacyjny sondy, to Mongoose V taktowany zegarem 12 MHz. Taka częstotliwość wystarcza, aby dystrybuować komendy do podsystemów, przetwarzać dane z instrumentów badawczych i wysyłać informacje na Ziemię. CPU wyposażono również w autonomiczne procedury pozwalające reagować na problemy, w tym przełączać się na systemy zapasowe oraz kontaktować się z operatorem na Ziemi.

Jaki jest kolejny cel wyprawy? Lot do pasa Kuipera. A może i dalej – poza Układ Słoneczny, goniąc dwa relikty ziemskiej technologii – Voyagera 1 i Voyagera 2.

POLECAMY

ADFS – RELACJE ZAUFANIA FEDERACJI (CZ. 3)

Relacje zaufania federacji jako alternatywa dla nadawania dostępu do zasobów użytkownikom obcych usług Active Directory oraz sposób na łatwą implementację rozwiązania w ramach infrastruktury IT – **s. 25**

STANDARYZACJA BEZPIECZEŃSTWA W CHMURZE

Najistotniejsze wytyczne opisane w normie ISO/IEC 27018:2014 oraz zasady dotyczące funkcjonowania normy w ramach polskiego porządku prawnego – **s. 40**

PACKER – SZYBKIE TWORZENIE MASZYN WIRTUALNYCH

Możliwości darmowego i łatwego w obsłudze narzędzia ułatwiającego tworzenie maszyn wirtualnych. Przygotowywanie identycznych obrazów VM dla takich systemów wirtualnych jak: EC2 Amazon, VirtualBox, Open Stack – **s. 62**

TESTY

Stormshield SN900 – test wydajnego, skutecznego i dostosowanego do polskich realiów UTM-a, wyposażonego w dedykowany filtr URL ze zlokalizowanym zestawem kategorii – **s. 47**

BIG DATA

DUŻE ZBIORY DANYCH – WYZWANIA DLA BIZNESU

Zmiany wynikające z dynamicznego przyrostu danych i konieczności przetwarzania dużych ilości informacji – **s. 33**

IT professional

ADRES REDAKCJI
ul. T. Kościuszki 29/2
50-011 Wrocław
tel. (+71) 797 28 46, faks (+71) 797 28 16

ADRES INTERNETOWY
www.it-professional.pl
redakcja@it-professional.pl

REDAKTOR NACZELNY
Artur Cieślik
artur.cieslik@it-professional.pl

REDAKTOR PROWADZĄCY
Jerzy Michalczyk
jerzy.michalczyk@it-professional.pl

REDAKTOR
Sebastian Kuniszewski
sebastian.kuniszewski@it-professional.pl

KOREKTA
Bogusława Otfinowska

PROJEKT GRAFICZNY I SKŁAD
Marcin Szewczyk
dtp@presscom.pl

WYDAWCA
PRESSCOM Sp. z o.o.
ul. T. Kościuszki 29
50-011 Wrocław
www.presscom.pl
biuro@presscom.pl

PREZES ZARZĄDU
Paweł Podkański

DYREKTOR WYDAWNICZY
Przemysław Golis

REKLAMA
Mikołaj Marzec
tel. (+71) 797 48 05 / tel. kom. (+606) 792 942
mikolaj.marzec@presscom.pl

Agata Szymonis-Szymanowska
tel. kom. (+666) 050 969
agata.szymanowska@presscom.pl

Małgorzata Salczyńska
tel. kom. (+604) 174 172
malgorzata.salczynska@presscom.pl

Magdalena Koczerga
tel. kom. (+728) 980 807
magdalena.koczerga@presscom.pl

PATRONATY
Jacek Śmieszek-Świętalski
tel. (+71) 797 28 30
jacek.smieszek@presscom.pl

PRENUMERATA
tel. (+71) 797 28 34
prenumerata@it-professional.pl
www.it-professional.pl
Bank Zachodni WBK S.A.
96 1090 1522 0000 0001 0162 2418

Nakład: 6000 egz.
Okładka: Aneta Szczęsna

Wydawca jest członkiem Izby Wydawców Prasy

Niszczenie na poziomie

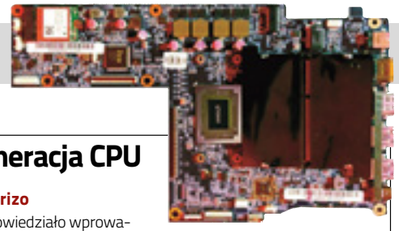
Rexel Auto+300M

Rexel Auto+300M to niszczarka dokumentów wyposażona w system automatycznego niszczenia. Do podajnika można włożyć jednorazowo nawet 300 kartek A4. Urządzenie wyposażono w samooczyszczające się ostrza i kosz na ścinki o pojemności 40 litrów mieszczący 500 pociętych kartek A4. Niszczarka tnie dokumenty wraz z zszywkami i spinaczami biurowymi na fragmenty o rozmiarach 2×15 mm, co odpowiada standardowi bezpieczeństwa P-5 (zalecanemu do dokumentów zawierających tajne informacje). Urządzenie niszczy też płyty CD i karty płatnicze. Model ma czterocyfrową blokadę komory podajnika, zapewniającą bezpieczne niszczenie dokumentów bez konieczności nadzoru. **rexel-polska.pl**

Kompletna digitalizacja

Skanery Fujitsu

Fujitsu zaprezentowało trzy nowe modele skanerów dokumentowych: SP-1120, 1125 i 1130. Są w stanie rejestrować obraz z prędkością 20, 25 lub 30 stron na minutę (druk dwustronny A4 w kolorze, 200/300 dpi). Wszystkie urządzenia z serii SP wyposażone są w sterownik PaperStream IP oraz oprogramowanie poprawiające jakość rejestrowanego obrazu. Sterownik obsługuje standardy TWAIN i ISIS, automatycznie wykrywa rozmiar dokumentu, jego rodzaj (jednostronny/dwustronny) oraz ułożenie. W pakiecie oprogramowania znajdują się także ABBYY FineReader Sprint oraz Presto! PageManager. **fujitsu.com**



6. generacja CPU

AMD Carrizo

AMD zapowiedziało wprowadzenie na rynek procesora szóstej generacji przeznaczonego do notebooków, będącego układem APU (Accelerated Processing Unit) w formie SoC (System-on-Chip). Układ oferuje sprzętowe wsparcie dla dekodowania HEVC/H.265, konstrukcję zgodną ze specyfikacją HSA 1.0 (architektura systemów heterogenicznych) oraz implementację technologii ARM TrustZone. Nowy procesor może zawierać nawet 12 rdzeni obliczeniowych – cztery dla CPU i osiem GPU, które wykorzystują mikroarchitekturę AMD Excavator oraz Graphics Core Next (GCN) firmy AMD. **amd.com**

Dla systemów SCADA

Check Point 1200R

Brama bezpieczeństwa firmy Check Point może być stosowana w takich miejscach jak zakłady przemysłowe, odległe podstacje elektryczne i elektrownie. Urządzenie oferuje ochronę systemów SCADA dzięki ponad 500 poleceniom SCADA i parametrom Firewalla Check Point, systemowi Application Control Software Blades oraz ponad 200 sygnaturom IPS dostępnym wyłącznie dla systemów SCADA. 1200R obsługuje szereg protokołów ICS/SCADA, między innymi: Modbus, MMS, DNP3, IEC 60870-5-104, IEC 61850, ICCP, OPC, BACnet, Profinet, Siemens Step7 i inne. **checkpoint.com**

Asus RT-AC3200 to trzyzakresowy router Wi-Fi wyposażony w sześć zewnętrznych anten działających w konfiguracji 3×3, które zasilają dwa pasma 802.11ac 5 GHz. Każde z nich pozwala uzyskać prędkość rzędu 1300 Mbit/s (1,3 Gbit/s). Router wykorzystuje też technologię Broadcom TurboQAM, która przyspiesza połączenie w paśmie 802.11n 2,4 GHz z 450 Mbit/s do 600 Mbit/s. Ponadto technologia uniwersalnego formowania wiązki AiRadar oraz regulacja częstotliwości radiowej (RF) wzmacniają sygnał bezprzewodowy i zwiększają jego pokrycie. Adaptacyjny QoS samodzielnie przydziela priorytety i przepustowość urządzeniom czy aplikacjom. Traffic Analyzer monitoruje połączenie, a AiProtection korzystająca z technologii Trend Micro dba o bezpieczeństwo sieci. Urządzenie wyposażono w cztery porty 1 GbE LAN oraz jeden port 1 GbE WAN, jeden port USB 3.0 i jeden port USB 2.0. **asus.com**

NETGEAR EX3800 to wzmacniacz sygnału Wi-Fi zaprojektowany w technologii PowerLine. Do transmisji danych wykorzystuje istniejącą instalację elektryczną. Urządzenie wzmacnia i rozszerza zasięg sygnału Wi-Fi w sieci, redukując martwe punkty. Zapewnia obsługę Wi-Fi z prędkością do 750 Mbps zgodnie ze standardem 802.11ac, ma dwie zewnętrzne anteny dla zwiększenia zasięgu sieci. EX3800 może również pełnić rolę hotspota. Wystarczy przełączyć wzmacniacz sygnału w tryb punktu dostępowego i podłączyć kabel sieciowy do portu Ethernet. **netgear.pl**

Monitoring wizyjny

Panasonic True 4K

Panasonic przedstawi zintegrowany system monitoringu wideo 4K. Oprócz kamery kopułkowej True 4K (WV-SFV781L) w ofercie firmy znajdzie się sieciowy rejestrator wideo (NVR), a także monitory 4K do tworzenia ścian wizyjnych. Kamera może objąć teren czterokrotnie większy niż kamera o jakości 1080p oraz dziewięciokrotnie większy niż urządzenie o rozdzielczości 720p. Kamera oferuje ponadto szerokie pole widzenia o kącie od 16° do 100°. Połączenie matrycy o wielkości 1/1,7" z obiektywem F1,6 daje możliwość pracy przy oświetleniu na poziomie 0,3 luksa dla obrazu kolorowego oraz 0,03 luksa dla obrazu czarno-białego. **panasonic.com**

Z Androidem i Google Cast

Monitory Sony Bravia

Sony Professional Solutions wprowadza do sprzedaży 10 nowych modeli monitorów Bravia o przekątnych od 43" do 85", w tym pięć o rozdzielczości 4K. Cechuje je zgodność z rozwiązaniami digital signage opartymi na języku HTML5, tryb hotelowy oraz funkcje IP. Nowością jest zastosowanie w nich technologii Android i Google Cast. Wbudowana platforma HTML5 umożliwia tworzenie dynamicznych materiałów digital signage obejmujących tekst, grafikę, materiały wideo, sygnały wideo transmitowane na żywo czy telewizję IP oraz ich przesyłanie do monitorów na całym świecie. Tryb hotelowy pozwala dostosowywać zaawansowane ustawienia i funkcje do wymagań danego pomieszczenia. **sony.pl**

UTM z Wi-Fi

Cyberoam CR10wiNG

Nowy UTM firmy Cyberoam oferuje kompleksową ochronę sieci w małych i domowych biurach, a także oddziałach firm. Urządzenie wykorzystuje technologię identyfikacji użytkowników i pozwala administratorom na tworzenie polityk bezpieczeństwa na podstawie tożsamości poszczególnych użytkowników, a także na zarządzanie dostępem gości do sieci. CR10wiNG obsługuje wiele (maks. osiem) wirtualnych punktów dostępowych, które tworzą niezależne, odrębne sieci dla poszczególnych zespołów. Cyberoam CR10wiNG zapewnia przepustowość Firewalla na poziomie 400 Mbps i przepustowość UTM na poziomie 60 Mbps. Bezprzewodowe urządzenie obsługuje standardy 802.11 b/g/n oraz zapewnia do ośmiu punktów dostępu SSID. **cyberoam.pl**

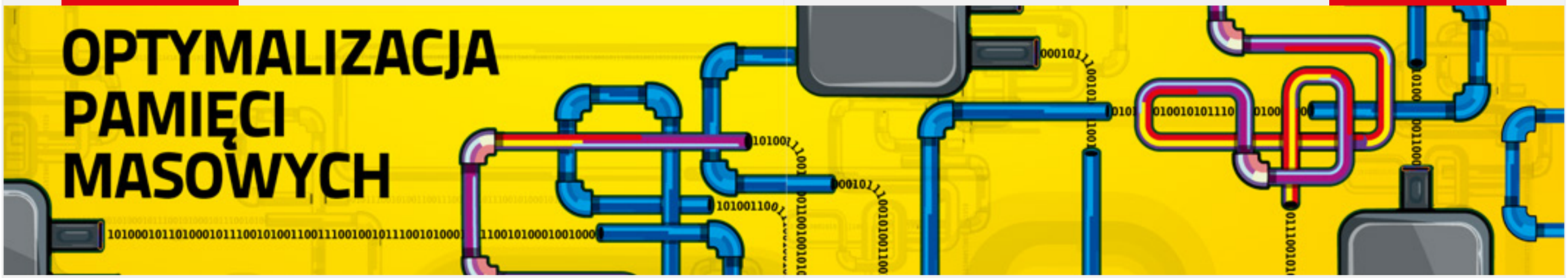
Android w A3

Samsung MultiXpress 7

Nowe urządzenie wielofunkcyjne MultiXpress 7 wyposażono w czterordzeniowy procesor (+DSDF) oraz system Android z Samsung Smart UX 2.0, który umożliwia użytkownikom podgląd i edycję plików z poziomu urządzenia przed wydrukiem, a także pozwala na pobieranie aplikacji usprawniających procesy biznesowe ze sklepu z oprogramowaniem do drukarek Samsung. Urządzenie zapewnia druk w w rozdzielczości do 1200 dpi. Wydruk pierwszej strony dokumentu cz.-b. zajmuje 3 sekundy, a kolorowego – 4,5. Wbudowany skaner przetwarza do 120 jednostronnych dokumentów na minutę i do 240 stron dokumentów dwustronnych. **samsung.pl**

Ricoh SP 6430DN to nowa drukarka monochromatyczna A3. Urządzenie cechuje niski pobór energii i wskaźnik TEC (Typical Electricity Consumption) – 2.3 kWh. W trybie uśpienia zużycie energii nie przekracza 1 W. SP 6430DN wyposażono w standardzie w kasetę na 500 arkuszy (z możliwością rozbudowy do pojemności maks. 2100 kartek). Urządzenie drukuje z prędkością 38 stron na minutę na papierach o gramaturze od 52 do 220 g/m², a wydruk pierwszej strony jest gotowy po 6,5 sekundy. **ricoh.com**

Powerline Green 33 Lite to zmodernizowana linia zasilaczy awaryjnych klasy online firmy Ever. Przeznaczono je do współpracy ze szczególnie wrażliwymi odbiornikami: serwerami, komponentami sieci komputerowych i systemami obróbki danych zasilanymi z trójfazowej sieci elektroenergetycznej. UPS-y zapewniają możliwość kompensacji mocy biernej przez wewnętrzne bloki zasilacza, tryb pracy hybrydowej oraz dynamiczny algorytm sterowania chłodzeniem. Powerline Green 33 Lite pozwalają ponadto na analizę parametrów środowiskowych, tryb pracy ECO, skalowalności mocy oraz czasu pracy autonomicznej. Konstrukcja umożliwia również szybką wymianę baterii. W serii Lite zmieniono panel frontowy, który nie jest już dzielony na mniejsze części przykręcane oddzielnie, a panel sterujący oraz diagram znajdują się w górnej lewej części UPS-a i są nieruchome. Dzięki tej zmianie urządzenie jest niższe, co ułatwia jego ustawienie i montaż. **ever.eu**



ZWIĘKSZANIE WYDAJNOŚCI MACIERZY DYSKOWYCH

Mechanizmy dostępne w macierzach dyskowych, ich budowa oraz protokoły są stale modyfikowane w miarę pojawiania się nowych potrzeb. Jednym z ciekawszych rozwiązań są technologie wykorzystujące dyski SSD do zwiększania wydajności przy jednoczesnym uwzględnianiu poziomu ponoszonych kosztów.

Michał Kaźmierczyk

Przez wiele lat rynek macierzy dyskowych skupiał się głównie (choć nie tylko) wokół urządzeń do przechowywania kopii zapasowych oraz plików przechowywanych w dużych bazach danych. Sytuacja znacząco zmieniła się wraz z wprowadzeniem i upowszechnieniem się wirtualizacji oraz z obserwowanym w ostatnich latach drastycznym wzrostem wolumenu gromadzonych danych.

Przyjrzyjmy się bliżej zagadnieniu wirtualizacji. Jak wiadomo, podstawowym jej założeniem jest konsolidacja przetwarzania, co oznacza, że dążymy do zmieszczenia jak największej liczby systemów (wirtualnych maszyn) w ramach pojedynczego serwera fizycznego. Wirtualizacja wymaga jednak użycia współdzielonej macierzy, na której przechowywane będą dane wszystkich naszych wirtualnych maszyn. To z kolei implikuje konieczność zapewnienia przez storage nie tylko odpowiedniej pojemności, ale również wydajności i przepustowości pozwalających na obsługę jak największej liczby operacji wejścia-wyjścia. Im środowisko wirtualne jest bardziej skonsolidowane i używanych jest więcej maszyn wirtualnych przechowywanych na wspólnej macierzy dyskowej, tym większe są wymagania dotyczące wydajności tego typu urządzeń.

FASTCACHE – ZASTOSOWANIE I EFEKTYWNOŚĆ

EMC podaje przykładowe środowiska, na których przeprowadzono testy mechanizmów FastCache. Po włączeniu cache'u **dla MS SQL Server w środowisku OLTP** (Online Transaction Processing) udało się podwoić liczbę jednoczesnych użytkowników, przy zastosowaniu tej samej liczby dysków mechanicznych. Jednocześnie odnotowano skrócenie czasu odpowiedzi z 40 do 5 sekund.
Z kolei **dla środowiska VMware View z włączoną pulą desktopów** typu linked-clone udało się zredukować liczbę operacji I/O na dyskach mechanicznych o 99% w sytuacji zwiększonego zapotrzebowania na I/O, podczas jednoczesnego uruchamiania dużej liczby desktopów (Boot Storm).

> WYDAJNOŚĆ SIECI SAN

Wydajność operacji storagowych zależy od zastosowanych w serwerach adapterów SAN oraz takich czynników jak:

- protokół sieci SAN,
- przepustowość sieci,
- konstrukcja macierzy,
- rodzaj grupy RAID,
- zastosowany typ dysków,
- inne technologie zwiększające wydajność rozwiązania.

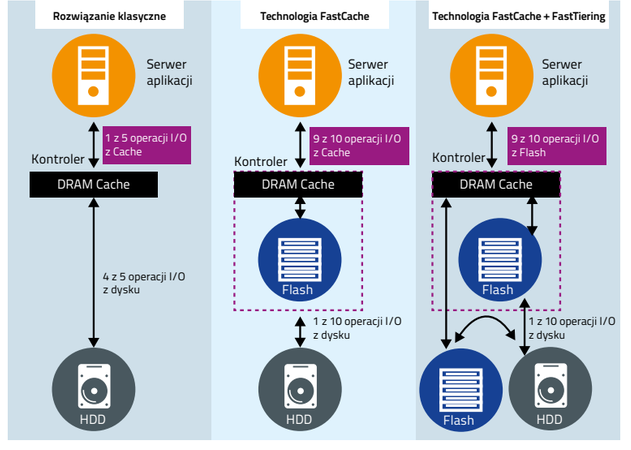
Pierwsze cztery czynniki omówimy tylko skrótowo. Skupimy się natomiast na dwóch ostatnich punktach – stosowanych typach dysków oraz technologiach zwiększających wydajność, a w szczególności na rozwiązaniach oferowanych przez EMC, czyli technologii Fast Cache i Fast-VP.

Protokół SAN i przepustowość to elementy w pewien sposób ze sobą powiązane. Najczęściej mamy do czynienia z protokołami iSCSI lub Fibre Channel, ewentualnie FCoE. Na ten moment, dla protokołów bazujących na Ethernecie, używamy przepustowości 1 i 10 Gbit/s. W przypadku FC dostępne są karty i urządzenia obsługujące przepustowości 4, 8 i 16 Gbit/s.

Można stwierdzić, że 10 Gbit/s dla iSCSI oraz 8 Gbit/s w przypadku FC to w większości przypadków wartości wystarczające do stosowania w średniej i dużej wielkości organizacjach. Rzadko spotyka się sieci SAN na tyle mocno obciążone, aby wysycone było całe dostępne pasmo. Zwłaszcza że w wielu przypadkach w organizacjach wykorzystywany jest load balancing oraz dokonywana jest agregacja linków. Rozważając punkt trzeci, czyli konstrukcje macierzy, należy mieć na myśli typy Active-Passive, Active-Active i ALUA. Wymienione tryby pracy mają istotne znaczenie nie tylko w zakresie zwiększania dostępnego pasma poprzez load balancing, ale również w zapewnianiu odpowiedniej wydajności samej macierzy poprzez możliwość rozłożenia przetwarzania na dwa kontrolery (w przypadku macierzy Active-Active i ALUA).

Kolejny wspomniany czynnik, czyli grupa RAID, to parametr, który najczęściej jest wąskim gardłem wydajnościowym

WZROST WYDAJNOŚCI OBSŁUGI I/O DZIĘKI ZASTOSOWANIU TECHNOLOGII FASTCACHE I FASTVP



KROK PO KROKU

TWORZENIE WIRTUALNEJ SIECI AZURE

A01. Proces tworzenia sieci wirtualnej w chmurze Azure rozpoczynamy od odnalezienia odpowiedniej usługi, czyli w naszym wypadku **Sieci wirtualne**.

B02. W ramach portalu zostajemy przeniesieni do listy dostępnych **Sieci wirtualnych**. O ile wcześniej nie konfigurowaliśmy żadnych sieci, lista powinna być pusta. Aby utworzyć nową sieć, klikamy przycisk **Dodaj**.

C03. Kreator tworzenia nowej sieci wirtualnej wymaga określenia sporej ilości informacji. Na wstępie definiujemy nazwę sieci np. **NorthEurope-VNet**.

C04. Dodatkowo definiujemy przestrzeń adresową. Powinna być ona na tyle duża, aby pomieścić wszystkie możliwe podsieci, jakie będą dostępne w ramach lokalizacji w chmurze.

C05. W przypadku gdy posiadamy większą liczbę subskrypcji Azure, wskazujemy, do której z nich ma być przypisana tworzona sieć.

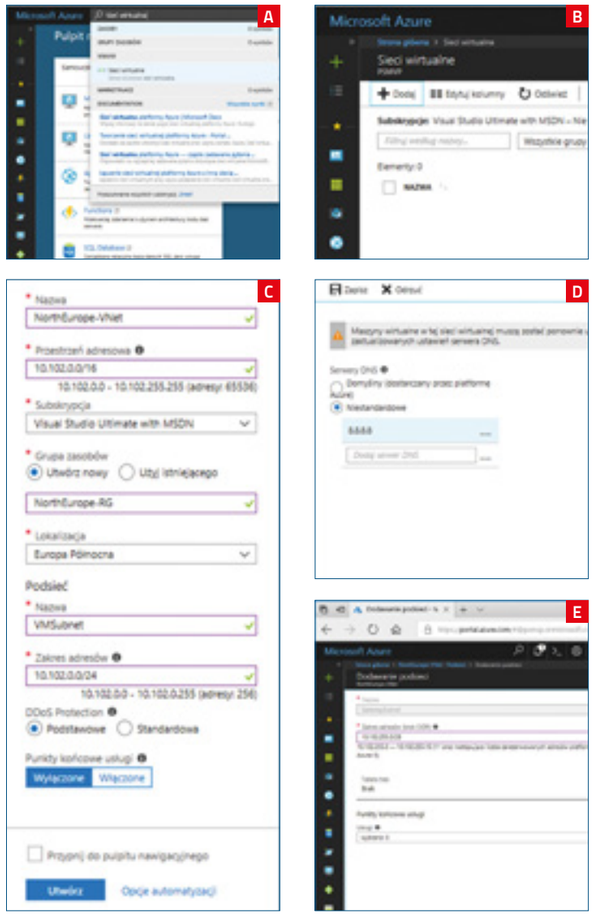
C06. Tworzymy nową grupę zasobów albo wskazujemy istniejącą, jeżeli wcześniej została już utworzona.

C07. Wybieramy lokalizację (w ramach którego centrum danych będą tworzone zasoby).

C08. Ostatecznie definiujemy podstawową podsieć, czyli podajemy jej nazwę oraz zakres adresów IP zawierających się we wcześniej określonej przestrzeni adresowej.

C09. Działania zatwierdzamy przyciskiem **Utwórz**.

D10. Po utworzeniu usługi sieci wirtualnej opcjonalnie wskazujemy własne serwery DNS, które będą używane przez maszyny wirtualne wdrażane w ramach utworzonej sieci. W tym celu przechodzimy do edycji sieci wirtualnej i z ustawień wybieramy pozycję **Serwery DNS**.



E11. Do sieci wirtualnej dodajemy kolejną podsieć – podsieć bramy. Z ustawień sieci wirtualnej wybieramy **Podsieci | Podsieć bramy**. W ramach tworzonej podsieci określamy zakres adresów, który również będzie pochodził z wcześniej zdefiniowanej przestrzeni adresowej. Domyślnie nazwa podsieci ma wartość **GatewaySubnet**. Jest to wymagane do identyfikacji podsieci bramy przez platformę Azure.

Drugim sposobem konfiguracji jest wykorzystanie konsoli Windows PowerShell wraz z dedykowanymi modułami Azure Resource Manager, czyli AzureRM. Aby to rozwiązanie było możliwe, konieczna jest aktualizacja modułu PowerShellGet oraz zainstalowanie wspomnianego zestawu modułów AzureRM:

```
Install-Module PowerShellGet -Force
Install-Module -Name AzureRM `
-AllowClobber
```

Docelowo wystarczy podłączyć się do zasobów w chmurze poleceniem:

```
Connect-AzureRmAccount
```

Pracę ze skryptami i siecią wirtualną Azure rozpoczynamy od utworzenia nowej grupy zasobów platformy Azure (o ile jeszcze takiej nie posiadamy). W tym celu wykorzystujemy cmdlet **New-AzureRmResourceGroup**, dla którego określamy nazwę grupy oraz lokalizację, czyli wskazanie, z którego centrum danych platformy Azure chcemy korzystać, na przykład Europa Północna:

```
New-AzureRmResourceGroup -Name `
'NorthEurope-RG' -Location `
'North Europe'
```

Następnie tworzymy minimum dwie podsieci wirtualne. Jedna z nich będzie przeznaczona do obsługi maszyn wirtualnych. Na przykład będzie to klasyczna podsieć z prefiksem maski `/24`:

```
$Subnet1 = New-AzureRmVirtualNetwork-
SubnetConfig -Name 'VMSubnet' `
-AddressPrefix 10.102.0.0/24
```

Druga podsieć będzie obsługiwała usługę bramy sieci wirtualnej. Ważne, aby podsieć bramy posiadała dokładnie określoną nazwę o wartości **GatewaySubnet**. Jest to informacja dla platformy Azure, że ta podsieć będzie obsługiwać usługę Azure Gateway. Dodatkowo niniejszą podsieć można odpowiednio zmniejszyć, na przykład stosując prefiks maski `/27` lub `/28`. Przykładowo:

KROK PO KROKU

TWORZENIE BRAMY SIECI WIRTUALNEJ

A01. Zanim rozpoczniemy proces tworzenia bramy sieci wirtualnej, tworzymy niezbędny publiczny adres IP. W tym celu wyszukujemy usługę o adekwatnej nazwie **Publiczne adresy IP** i przechodzimy do kreatora konfiguracji.

A02. W ramach kreatora określamy tylko nazwę usługi, wartości pozostałych parametrów mogą pozostać domyślne.

B03. Rozpoczynamy proces tworzenia nowej bramy sieci wirtualnej. W tym celu znajdujemy element platformy Azure o nazwie **Virtual Network Gateway**.

B04. W ramach kreatora tworzenia bramy sieci wirtualnej podajemy jej nazwę, np. **NorthEurope-VGW**.

B05. Zostawiamy domyślny typ bramy na pozycji VPN oraz typ sieci VPN oparty na trasie.

B06. Określamy wartość jednostki SKU, czyli parametry związane z obciążeniem i przepustowością bramy. W testowym przypadku wybieramy pozycję **Podstawowe**, co będzie wiązało się z ograniczeniem przepustowości do 100 Mb/s. Dla większych wdrożeń możliwe jest zastosowanie pakietów:

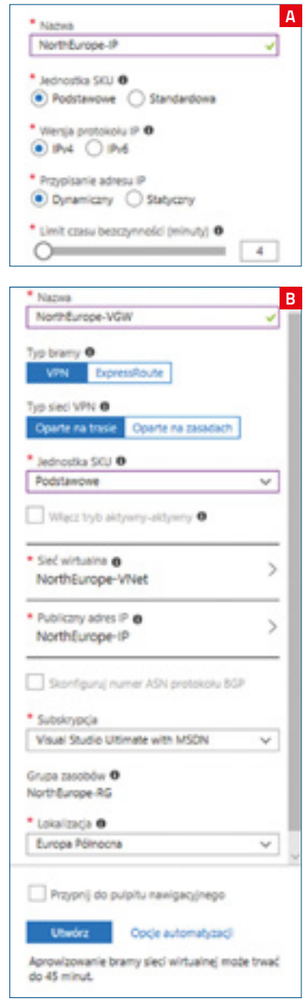
- VpnGw1 – 650 Mb/s
- VpnGw2 – 1 Gb/s
- VpnGw3 – 1,25 Gb/s

B07. Następnie wskazujemy utworzoną w poprzednim kroku sieć wirtualną **NorthEurope-VNet**.

B08. Wskazujemy wcześniej przygotowany publiczny adres IP.

B09. Weryfikujemy pozostałe parametry, czyli wykorzystywaną subskrypcję, grupę zasobów oraz lokalizację Azure i kończymy proces, klikając **Utwórz**.

Proces generowania bramy jest operacją czasochłonną, która może potrwać nawet do kilkudziesięciu minut.



MACHINE LEARNING/DATA SCIENTIST (CZ. 9)

PYTHON, WIZUALIZACJA DANYCH

Biblioteki Seaborn pozwalają na wizualizację modeli statystycznych w prostszy sposób niż omawiany w poprzednich częściach kursu Matplotlib. Przedstawiamy możliwości i funkcje oferowane przez Seaborn oraz odpowiadamy na pytanie, dlaczego są one ważnym elementem w nauce specjalizacji data scientist.

Grzegorz Kubera

Bardzo często do wizualizacji danych wykorzystywane są biblioteki Matplotlib – oferują one duże możliwości, jednak trudno za ich pomocą tworzyć bardziej skomplikowane i niestandardowe wykresy. Żeby ułatwić sobie pracę i uzyskać atrakcyjne wizualnie efekty, warto doinstalować biblioteki Seaborn (Statistical Data Visualization Library), które są niejako nakładką na Matplotlib i współpracują z obiektami dataframe z bibliotek Pandas.

Seaborn z założenia mają umożliwić tworzenie atrakcyjnych wykresów w prostszy sposób niż Matplotlib. Jak wspomniano, głównie służą do wizualizacji modeli statystycznych. Z uwagi na to, że w poprzednich częściach kursu poznaliśmy Matplotlib, nauka Seaborn nie powinna być zbyt trudna. Klasycznie zaczynamy od przygotowania środowiska pracy. Uruchamiamy wiersz poleceń Anaconda Prompt z menu Start w Windows i wpisujemy komendę:

```
conda install seaborn
```

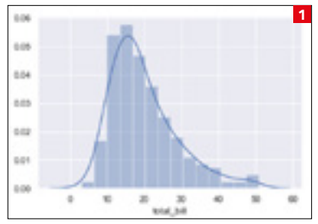
Jeśli wcześniej zainstalowane zostały już biblioteki NumPy i Matplotlib, nie trzeba instalować ich ponownie. W przeciwnym przypadku wpisujemy komendy:

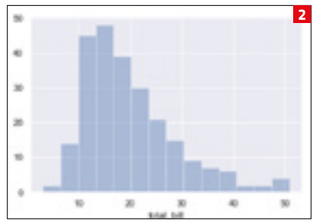
```
conda install numpy
conda install matplotlib
```

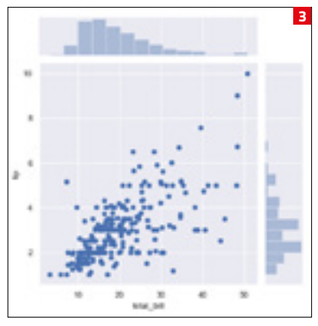
Możliwe jest, że wyświetli się komunikat o nowszej wersji Anacondy. W tym wypadku warto zainstalować aktualizację, wpisując polecenie:

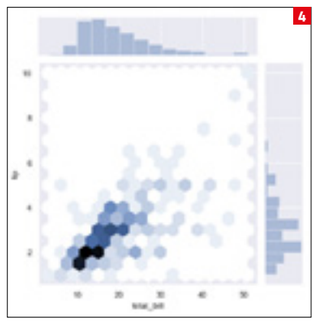
```
conda update -n base conda
```

Po zakończonej instalacji uruchamiamy Jupytera, wpisując:







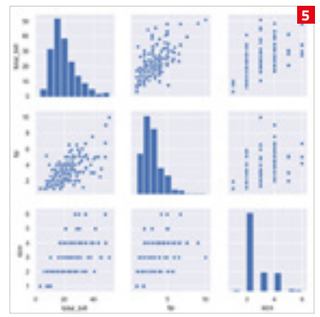


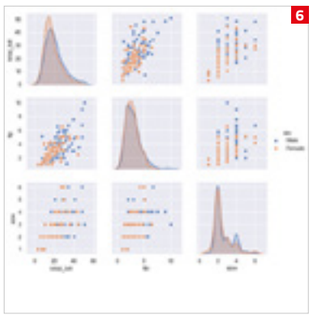

```
jupyter notebook
```

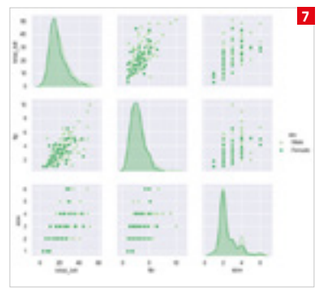
Następnie uruchamiamy Jupytera, otwieramy notatnik w Pythonie 3 i wpisujemy komendy:

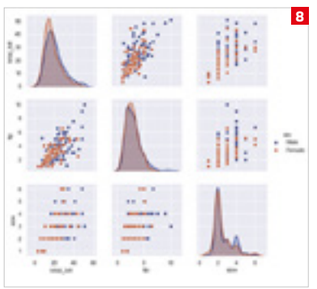
```
import seaborn as sns

%matplotlib inline

sns.set(color_codes=True)
```

Komenda `import` służy do importowania bibliotek do Jupytera, natomiast `%matplotlib inline` jest potrzebna do tego, aby można było nie tylko wpisywać kody związane z wykresami, ale również aby zobaczyć je w formie graficznej bezpośrednio w Jupyterze. Ostatnie z poleceń aktywuje style graficzne z Seaborn, które są atrakcyjniejsze niż style domyślne.









> WIZUALIZACJA DANYCH Z SEABORN

Kiedy środowisko pracy jest gotowe, możemy przejść do nauki funkcji i opcji dostępnych przez Seaborn. Co ciekawe, biblioteki te są oferowane z kilkoma wbudowanymi zestawami danych, dzięki czemu możemy je łatwo zaimportować i rozpocząć ćwiczenia.

Na potrzeby kursu importujemy zestaw o nazwie `tips` (z ang. napiwki). Dostępne są również inne zestawy, takie jak `iris` czy `titanic`. Aby zaimportować któryś z zestawów danych i następnie zapisać go jako obiekt `dataframe`, na którym będziemy pracować, wpisujemy w Jupyterze polecenie:

```
tips = sns.load_dataset('tips')
```

Teraz możemy sprawdzić, jak wygląda wybrany zestaw danych. W tym celu wpisujemy:

```
tips.head()
```

Uzyskany wynik powinien wyglądać jak w tabeli obok:

	total_bill	tip	sex	smoker	day	Time	size
0	16.99	1.01	Female	No	Sun	Dinner	2
1	10.34	1.66	Male	No	Sun	Dinner	3
2	21.01	3.50	Male	No	Sun	Dinner	3
3	23.68	3.31	Male	No	Sun	Dinner	2
4	24.59	3.61	Female	No	Sun	Dinner	4

Zestaw oferowany przez Seaborn dotyczy napiwków. Jak widać, mamy tutaj podział na kobiety i mężczyzn (`female` i `male`), informacje o wysokości całego rachunku zapłaconego w restauracji (`total_bill`) oraz o wysokości napiwku (`tip`), czy dana osoba pali papierosy, czy nie (`smoker`), w jakim dniu tygodnia odwiedziła restaurację (`day`), w jakiej porze (pora obiadowa, `dinner`) i jaka była liczba osób siedzących przy jednym stole (`size`).

Korzystając z tych danych, możemy stworzyć pierwszy wykres, w tym przykładzie obrazujący, jak rozkładają się kwoty rachunków. Chcemy zobaczyć, ile pieniędzy klienci najczęściej przeznaczają na posiłki. W tym celu wpisujemy:

```
sns.distplot(tips[,total_bill'])
```

Ta komenda pozwala stworzyć wykres z kolumny `total_bill` (rachunek) z zestawu danych o nazwie `tips`. Uzyskany wynik będzie wyglądać jak na **rys. 1**. Uwaga, ewentualne ostrzeżenie o niewłaściwie wpisanych funkcjach można zignorować – dotyczy innej biblioteki, StatsModels, i nie wpłynie na działania w tej części kursu.

Uzyskany wynik zawiera histogram oraz linię o nazwie KDE (Kernel Density Estimation – szacowana gęstość jądra, o której więcej w kolejnych częściach kursu). W tym momencie nie będziemy używać KDE, dlatego wyłączamy ją poleceniem:

```
sns.distplot(tips['total_bill'], \
kde=False)
```

Teraz wykres zawiera tylko histogram (**rys. 2**), który pokazuje rozkład dla wartości z kolumny `total_bill`. Wynika +

STACJE ROBOCZE

z niego, że większość rachunków wynosi od 10 do 20 dolarów.

Inny rodzaj wykresów to JointPlot – tworzy się, łącząc dwa różne zestawy danych. Przykładowo możemy porównać dane z kolumny total_bill z tymi z kolumny tip. W ten sposób ustalimy zależność pomiędzy rachunkiem a wysokością napiwku. Po wpisaniu w Jupyterze poniższej komendy uzyskamy rezultat jak na **rys. 3**:

```
sns.jointplot(x='total_bill',\
y='tip',data=tips)
```

Otrzymany wynik składa się z dwóch wykresów typu distplot, opracowanych wcześniej (na górze to total_bill, a z prawej tip), i znajdującego się między nimi wykresu łączonego jointplot, prezentującego dane w formie punktowej. Przy okazji widoczny jest trend – im wyższe rachunki za posiłek, tym wyższe są napiwki, co zresztą jest logiczne (napiwki wynoszą najczęściej 10–20% wartości zamówienia).

Funkcja do tworzenia wykresów łączonych pozwala jeszcze na wybranie rodzaju wykresu znajdującego się w środku. Służy do tego celu polecenie kind. Przykładowo możemy wpisać polecenie hex pozwalające na tworzenie rozkładu sześciokątnego. Efekt końcowy pokazano na **rys. 4**.

```
sns.jointplot(x='total_bill',\
y='tip',data=tips,kind='hex')
```

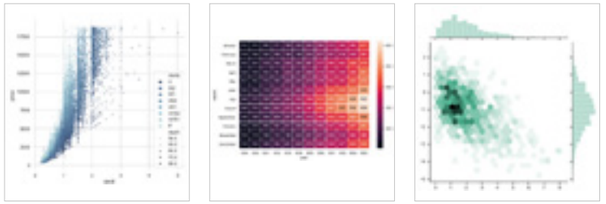
Jak widać, jeśli na wykresach hex w jednym obszarze znajduje się dużo punktów, sześcian staje się ciemniejszy, a jeśli ma mało punktów – jaśniejszy. To właśnie dobry przykład wizualizacji danych.

> PORÓWNYWANIE DANYCH

Kolejną funkcją, którą warto poznać, jest sprawdzanie powiązań pomiędzy poszczególnymi zestawami danych. Do tego celu wykorzystamy polecenie sns.pairplot(), które wskaże wszystkie powiązania dla kolumn numerycznych. Wpisujemy:

SEABORN – NOWOCZESNE WYKRESY

Na oficjalnej stronie Seaborn (**seaborn.pydata.org**) znajdziemy oprócz szczegółowej dokumentacji m.in. dwie użyteczne podstrony – API oraz Gallery. W API dostępne są wszystkie komendy dla Seaborn, wraz z wyjaśnieniami ich działania. W Gallery pokazano wiele przykładowych wykresów opracowanych z użyciem Seaborn. Łatwo zauważyć, że są to biblioteki, które już domyślnie oferują atrakcyjny i nowoczesny styl graficzny. Poniżej kilka przykładów.



```
sns.pairplot(tips)
```

Ta prosta komenda uwzględnia wszystkie powiązania i nie trzeba ich wskazywać pojedynczo (nie musimy podawać nazw kolumn). Warto dodać, że jeśli zbiór danych jest bardzo obszerny, na wizualizację efektu końcowego będziemy musieli czasami chwilę poczekać. W przypadku zbioru tips danych jest stosunkowo mało, dlatego efekty są gotowe niemal natychmiast i wyglądają jak na **rys. 5**. Funkcja pairplot() pozwala w szybki sposób zwizualizować dane, jakimi dysponujemy. Przedstawia je w formie wykresu punktowego, chyba że porównywane są ze sobą te same dane (np. size + size czy tip + tip) – wówczas tworzony jest histogram. Dodatkowo możemy dodawać parametr hue (odcień), aby jeszcze lepiej wizualizować dane. Odcień podajemy dla kategorii danych – czyli nie chodzi tu o dane numeryczne, lecz o nazwę kategorii, np. płeć. Żeby uzyskać wynik jak na **rys. 6**, wystarczy więc, że wpiszemy:

```
sns.pairplot(tips,hue='sex')
```

Teraz możemy zobaczyć inny przykład wykresów, w których wszystkie pomarańczowe punkty to kobiety, a niebieskie – mężczyźni. W przyszłości, kiedy będziemy tworzyć tego rodzaju wizualizacje danych, warto znać jeszcze polecenie palette, które pozwala dobrać paletę kolorów z dostępnych w bibliotece Seaborn. Aby skorzystać z odpowiedniej palety, wpisujemy w Jupyterze jej nazwę, np. Greens (**rys. 7**) lub dark (**rys. 8**) itp.:

```
sns.pairplot(tips,hue='sex',\
palette='Greens')
```

```
sns.pairplot(tips,hue='sex',\
palette='dark')
```

To oczywiście tylko kilka przykładów. Więcej informacji o zmiennych dotyczących kolorów i palet można znaleźć w dokumentacji Seaborn. W następnej części kursu poświęcimy nieco miejsca temu, jak tworzyć własne palety kolorów, oraz poznamy kolejne możliwości bibliotek.

Założyciel i dyr. generalny firmy doradczo-technologicznej, pełnił funkcję redaktora naczelnego w magazynach i serwisach informacyjnych z branży ICT. Dziennikarz z ponad 10-letnim doświadczeniem i autor książki nt. tworzenia start-upów.

sobie przyswoić, aby w przyszłości móc tworzyć oryginalne wykresy.

> SPECJALNE TYPY WYKRESÓW

Przy użyciu bibliotek Matplotlib możemy tworzyć również wiele wyspecjalizowanych wykresów, takich jak histogramy czy wykresy rozproszone. Do tych zadań w przyszłości (zaczynając od kolejnej części kursu) będziemy używać już bibliotek statystycznych dla Pythona – Seaborn. Niemniej w ramach ciekawostki i dla własnej wiedzy warto mieć świadomość, że również Matplotlib mają dość szerokie możliwości. Po wpisaniu poniższego polecenia otrzymamy wykres jak na **rys. 14**:

```
plt.scatter(x,y)
```

Następnie możemy stworzyć histogram, wykorzystując zakres następujących danych:

```
from random import sample
data = sample(range(1, 1000), 100)
plt.hist(data)
```

Dzięki temu uzyskamy wykres pokazany na **rys. 15**.

Z kolei poniższa komenda tworzy wykresy o nietypowym kształcie (**rys. 16**):

```
data = [np.random.normal(0, std, 100)
for std in range(1, 4)]
plt.boxplot(data,vert=True,patch_ar-
tist=True);
```

Podobne do trzech ostatnich zadania zostaną opisane w kolejnej części kursu. Tymczasem warto przyswoić sobie wszystkie komendy zaprezentowane w niniejszym artykule i stworzyć we własnym zakresie zestaw wykresów o różnym wyglądzie i z różnymi danymi.

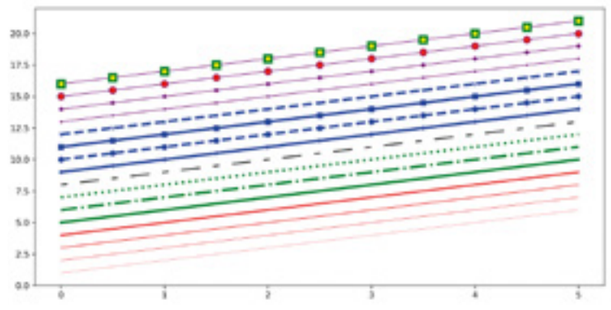
Założyciel i dyr. generalny firmy doradczo-technologicznej, pełnił funkcję redaktora naczelnego w magazynach i serwisach informacyjnych z branży ICT. Dziennikarz z ponad 10-letnim doświadczeniem i autor książki nt. tworzenia start-upów.

PERSONALIZOWANIE WYKRESÓW

Na potrzeby ćwiczeń warto tworzyć ciekawe wykresy, wyróżniające się stylem linii, kolorów czy znaczników. Poniżej zamieszczamy odpowiednie komendy i zrzut ekranowy w ramach inspiracji:

```
fig, ax = plt.subplots(figsize=(12,6))

ax.plot(x, x+1, color="red", linewidth=0.25)
ax.plot(x, x+2, color="red", linewidth=0.50)
ax.plot(x, x+3, color="red", linewidth=1.00)
ax.plot(x, x+4, color="red", linewidth=2.00)

ax.plot(x, x+5, color="green", lw=3, linestyle='-')
ax.plot(x, x+6, color="green", lw=3, ls='-.')
ax.plot(x, x+7, color="green", lw=3, ls=':')

line, = ax.plot(x, x+8, color="black", lw=1.50)
line.set_dashes([5, 10, 15, 10]) # format: line length, space length, ...

ax.plot(x, x+ 9, color="blue", lw=3, ls='-', marker='+')
ax.plot(x, x+10, color="blue", lw=3, ls='--', marker='o')
ax.plot(x, x+11, color="blue", lw=3, ls='-', marker='s')
ax.plot(x, x+12, color="blue", lw=3, ls='--', marker='1')

ax.plot(x, x+13, color="purple", lw=1, ls='-', marker='o', markersize=2)
ax.plot(x, x+14, color="purple", lw=1, ls='-', marker='o', markersize=4)
ax.plot(x, x+15, color="purple", lw=1, ls='-', marker='o', markersize=8, \
markerfacecolor="red")
ax.plot(x, x+16, color="purple", lw=1, ls='-', marker='s', markersize=8,
        markerfacecolor="yellow", markeredgewidth=3, markeredgecolor="green");
```

Oto uzyskane efekty:



Dodatkowo warto zapamiętać:

- dostępne style dla komendy linestyle: '-', '--', '-.', ':', 'steps'
- dostępne style dla znaczników: '+', 'o', '*', 's', ',', '.', '1', '2', '3', '4', ...

04. Examples of infographic pages of *IT Professional* magazine

Each issue of the monthly *IT Professional* contains five spreads that act as material separating individual sections of the magazine. The aim of these pages is to present the content in a loose and interesting way, a graphic style often referring to the subject discussed.

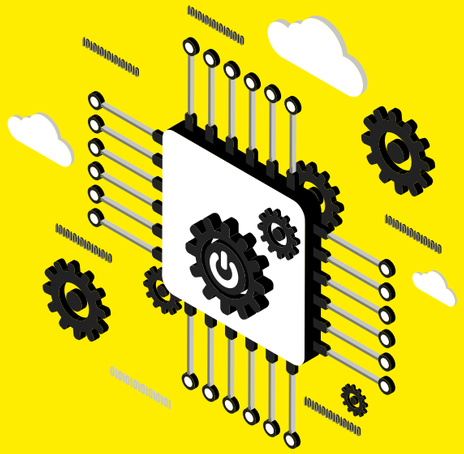
Scope of work:
– design
– layout
– typography
– graphic
– desktop publishing
– pre-press

↑ Click to move to Table of Contents

EWOLUCJA KRAJOBRAZU ZAGROŻEŃ SIECIOWYCH

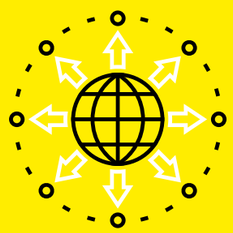
Nowe technologie i nowe zagrożenia to nierozłączna para. W którą stronę ewoluują jedne i drugie? Na co warto zwracać szczególną uwagę w tym roku? Wprowadzane rozwiązania oraz zmieniające się oczekiwania biznesu i użytkowników bezpośrednio związane są z cyfrową transformacją przedsiębiorstw. Warto być świadomym wyzwań dotyczących bezpieczeństwa IT w 2019 roku i wiedzieć, jak stawić im czoła. Sebastian Kuniszewski

Technologia to dziwna rzecz. Daje ci wspaniałe prezenty jedną ręką, a następnie wbija nóż w plecy drugą – pisał powieściopisarz i naukowiec C. P. Snow w „New York Timesie" w 1971 roku. Mimo upływu niemal półwiecza to zdanie jest ciągle aktualne. Każde nowe narzędzie czy technologia wprowadza nowe podatności, dając cyberprzestępcom możliwość wzbogacenia się, szpiegowania i manipulowania użytkownikami sieci. W którą stronę ewoluuje krajobraz zagrożeń sieciowych i jakich typów ataków możemy się spodziewać? Poniżej przedstawiamy kilka najważniejszych trendów.



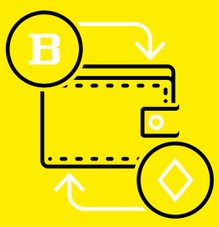
01
CRYPTOMINERY PRAWDZIWA ŻYŁA ZŁOTA

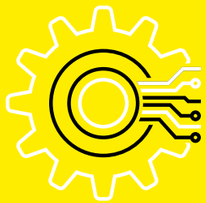
W roku 2018 cryptominery zdominowały rynek złośliwego oprogramowania, zastępując w ten sposób ransomware – ulubiony do tej pory sposób hakerów na nieuczciwe zarabianie pieniędzy. Według danych firmy Check Point w minionym roku aż 42% firm na całym świecie zostało zarażonych złośliwym oprogramowaniem wydobywającym kryptowaluty. Popularność tego typu ataków nie stanowi zaskoczenia, ponieważ są one łatwe do rozprzestrzeniania, trudne do wykrycia i mogą pozostać nierozpoznane przez wiele miesięcy, jednocześnie generując duże wpływy dla przestępców, przy znacznie mniejszym ryzyku niż ransomware. Cryptominery okazały się bardzo efektywne, dlatego specjaliści ds. bezpieczeństwa spodziewają się, że w 2019 roku będą one główną metodą ataku na firmy. Oprogramowanie wydobywające kryptowaluty jest ciągle usprawniane i można spodziewać się, że jego działanie zostanie rozszerzone na platformy chmurowe oraz urządzenia mobilne. Popularne rozwiązania to opcja zwiększenia nielegalnych zysków.



02
PLATFORMY MOBILNE – RUCHOME CELE

Urządzenia mobilne używane zarówno do celów służbowych, jak i przez osoby prywatne są coraz częstszym celem ataków. Mimo to bezpieczeństwo mobilne w organizacjach cały czas jest kwestią marginalną. W 2018 roku jedną z trzech najpopularniejszych złośliwych aplikacji był Lokibot – bankowy trojan przeznaczony na urządzenia z systemem Android kradnący dane i pobierający dalsze złośliwe oprogramowanie. We wrześniu 2018 analitycy Check Point odnotowali również wzrost o ponad 400% w użyciu cryptominerów na iPhone'y i urządzenia z systemem iOS. W związku z takimi działaniami spodziewany jest wzrost złośliwego oprogramowania mobilnego w bieżącym roku oraz pojawienie się odmian wszystko-w-jednym, łączących możliwości trojanów bankowych, keyloggerów i aplikacji ransomware, które dadzą atakującemu wiele sposobów na czerpanie korzyści z zarażonego urządzenia. Pewne jest też, że w dalszym ciągu będą odkrywane podatności w mobilnych systemach operacyjnych, umożliwiające atakującym uzyskanie dostępu do niezabezpieczonego urządzenia. Przykładem jest podatność Androida określana nazwą „man-in-the-disk", pozwalająca aplikacjom na atak poprzez użycie pamięci zewnętrznej smartfona lub tabletu.





03
ROZWÓJ UCZENIA MASZYNOWEGO

Rozwój technologii uczenia maszynowego i sztucznej inteligencji dramatycznie przyspieszyły identyfikację i przeciwdziałanie nowym zagrożeniom na przestrzeni ostatnich 20 miesięcy, pomagając likwidować nowe zagrożenia, zanim te były w stanie rozpowszechnić się na szeroką skalę. Jednakże popularyzacja i komercjalizacja technologii spowoduje, że cyberprzestępcy również zaczną z niej korzystać w celu skanowania sieci, znajdowania podatności i rozwijania trudniejszego do wykrycia złośliwego oprogramowania, które będzie miało większe szanse na pozostanie niezauważonym.

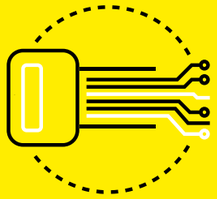
04
OBAWY O CHMURĘ

Skalowalność i elastyczność systemów chmurowych pozwalają organizacjom realizować projekty, o których mogły jedynie marzyć, używając tradycyjnych centrów danych. Jednak poziom wiedzy o bezpieczeństwie tego typu rozwiązań wciąż pozostaje niski. W listopadzie 2018 Check Point odkrył podatności w chmurowych platformach DJI – najpopularniejszego na świecie producenta dronów biznesowych i prywatnych. Pozwalały one atakującym na kradzież zapisów lotów, fotografii, informacji o lokalizacji w czasie rzeczywistym oraz danych konta, takich jak dane użytkownika i dane karty kredytowej. Wszystkie te działania mogły być realizowane bez wiedzy użytkownika. Mimo że podatności zostały wyeliminowane, zanim mogły zostać wykorzystane, powyższy przykład pokazuje, jak często o bezpieczeństwie myśli się dopiero po wdrożeniu technologii chmurowej, pozostawiając wrażliwe dane i aplikacje bez ochrony przed atakami hakerskimi.

Można przewidywać, że w ciągu bieżącego roku próby hakowania i przejmowania kont chmurowych staną się częstsze, ponieważ coraz więcej firm używa aplikacji w modelu SaaS oraz skrzynek w cloudowych systemach pocztowych (m.in. Office 365, GSuite i OneDrive). Z tego powodu firmy muszą być zdolne zapobiegać najczęściej spotykanym atakom na te platformy oraz szkolić pracowników w rozpoznawaniu prób wyłudzania danych (phishing).

05
OBAWY O BEZPIECZEŃSTWO NARODOWE

W ostatnich latach rządy większości państw zaczęły przejmować się cyberzagrożeniami wymierzonymi w infrastrukturę administracji publicznej i samorządowej oraz wysoką wrażliwością kluczowych zasobów (np. sieci elektrycznych). Wiele krajów stworzyło odpowiednie organy mające na celu ochronę i przygotowanie się na ewentualne ataki tego typu. Jak zwracają uwagę eksperci Check Point, w ostatnich latach zaobserwowano również ataki przygotowane przez



rządy wymierzone we własnych obywateli (np. sponsorowany przez rząd Iranu atak Domestic Kitten).

Natomiast nie odnotowano jeszcze ataków osób prywatnych na krytyczną infrastrukturę państwową w celu wywołania masowego zniszczenia. Mimo to wiele krajów deklaruje prowadzenie działań mających na celu zwiększanie skuteczności własnych technik cyberwojennych. W tym kontekście szpiegostwo cyfrowe i prywatność obywateli pozostaną szczególnie gorącym tematem, zwłaszcza że dowiedziono, że takie działania mają wpływ na wynik wyborów (afera z udziałem firmy Cambridge Analytica i serwisem społecznościowym Facebook oraz prezydenckimi wyborami w USA).

06
NANOAGENCI BEZPIECZEŃSTWA

W coraz większej liczbie przedsiębiorstw podłączane są do sieci podatne na ataki urządzenia IoT. Jednocześnie często zapomina się o aktualizowaniu i wzmacnianiu procedur bezpieczeństwa w celu poprawy ochrony firmowych sieci i urządzeń. Coraz liczniejsze urządzenia IoT i ich łączność z platformami chmurowymi to słabe ogniwo infrastruktury bezpieczeństwa.

W ciągu najbliższych dwóch lat fizyczna architektura będzie coraz szybciej przenosić się do chmury, co pozwoli na lepszą jej skalowalność w zależności od potrzeb. Urządzenia takie jak smartfony, autonomiczne pojazdy, czujniki IoT, sprzęt medyczny i inne będą łączyły się z chmurą za pośrednictwem internetu. Krytyczne stanie się zapewnienie bezpieczeństwa w świecie połączonych ze sobą urządzeń i powstrzymanie nowych zagrożeń, które mogą się niezauważalnie rozprzestrzeniać. Eksperci ds. bezpieczeństwa Check Point zapowiadają pojawienie się nowej generacji zabezpieczeń wykorzystujących nanoagentów bezpieczeństwa – niewielkie wtyczki, które będą mogły współpracować z dowolnym urządzeniem i systemem operacyjnym w dowolnym środowisku – od kamer bezpieczeństwa począwszy, poprzez urządzenia IoT, aż po mikrousługi w chmurze. Nanoagenty będą w stanie kontrolować każdy parametr przekazywany do urządzenia i do chmury, dodatkowo łącząc się z globalnym, inteligentnym i sterowanym przez mechanizmy sztucznej inteligencji systemem bezpieczeństwa zapewniającym ochronę i pozwalając podejmować decyzje w czasie rzeczywistym.

Podczas gdy innowacje w dalszym ciągu będą przynosić nowe okazje do przyspieszenia rozwoju biznesu, cyberprzestępcy będą szukać sposobów, aby wykorzystać je dla własnych celów. Żeby nadążyć za rozwojem wydarzeń, organizacje powinny aktywnie działać, nie pozostawiając żadnych elementów niechronionych i poza kontrolą. W przeciwnym wypadku mogą stać się jedną z ofiar zaawansowanych, szczegółowo zaplanowanych globalnych ataków.

ZASADY KONSENSUSU*

A SKALOWALNOŚĆ I WYDAJNOŚĆ SIECI

Blockchain oferuje wiele atrakcyjnych funkcji i możliwości, ma jednak też pewne ograniczenia. Świadomość ich istnienia i zrozumienie są istotne dla identyfikacji obszarów zastosowań łańcucha bloków i ustalania przez firmy priorytetów inwestycyjnych. Sebastian Kuniszewski

Wykorzystanie technologii łańcucha bloków umożliwia tworzenie zupełnie nowej klasy aplikacji rozproszonych i może mieć ogromne znaczenie dla innowacji w obszarze procesów biznesowych. Jednak intensywność obliczeniowa potrzebna do synchronizacji danych w sieciach blockchain ogranicza w pewnym stopniu skalowalność tego typu rozwiązań i może generować opóźnienia w przetwarzaniu transakcji. Warto wiedzieć, że większość platform blockchain ma znacząco niższą wydajność niż tradycyjne systemy transakcyjne (patrz **ramka** na stronie obok).

DELOITTE'S 2018 GLOBAL BLOCKCHAIN SURVEY

Z badania pt. „Breaking blockchain open. Deloitte's 2018 global blockchain survey", które objęło ponad 1000 menedżerów wykonawczych czołowych firm z Europy Zachodniej, Ameryki Północnej i Chin, wynika, że 39% z nich zainwestuje w tym roku ponad 5 mln dol. w technologię blockchain. 65% badanych deklaruje, że zainwestuje ponad 1 milion dolarów, a 84% z nich uważa, że blockchain jest już wystarczająco skalowalny i może mieć zastosowanie w głównym nurcie ich biznesu.

CZYM JEST KONSENSUS

Konsensus jest najważniejszym elementem każdej sieci blockchainowej – to sposób, w jakim wszystkie węzły w sieci podejmują decyzję o tym, czy konkretna operacja (np. przesłanie informacji lub tokenów) może być zaakceptowana i dodana do bloku danych i w związku z czym być niepodważalna. Osiągnięcie konsensusu nie wymaga udziału fizycznych osób ani instytucji, jest efektem automatycznego działania zaimplementowanego kodu. Od konsensusu zależy też, jak bardzo bezpieczna jest dana sieć blockchainowa oraz jak szybko będą zatwierdzane w niej kolejne operacje i ile to będzie kosztować jej użytkowników.

Sposób osiągania konsensusu w sieciach blockchainowych jest głównym problemem w zakresie osiągania stanu optymalnego, rozumianego jako maksymalne bezpieczeństwo sieci przy jednoczesnie możliwie jak najniższych kosztach i jak najwyższej prędkości zatwierdzania bloków (czyli wydajności sieci). W tabeli opisano najważniejsze cechy różnych typów konsensusu, a wybór konkretnego z nich powinien być podjęty po szczegółowej analizie potrzeb związanych z danym systemem. Bezpieczeństwo rośnie wraz z liczbą węzłów autoryzujących operacje, jednak im większa liczba węzłów, tym dłużej trwa weryfikacja każdej kolejnej operacji. Oznacza to, że sieć zawierająca więcej węzłów będzie zatwierdzała mniej operacji, innymi słowy, każde zwiększenie bezpieczeństwa lub wydajności będzie się odbywało kosztem drugiego parametru.

Cały czas trwają intensywne poszukiwania metody konsensusu, w której wydajność i bezpieczeństwo sieci będą na najwyższym poziomie. Jednym z obiecujących projektów testujących tzw. metody mieszane jest Zilliqua, w którym metodę PoW zmodyfikowano w taki sposób, że węzły są grupowane w ramach mniejszych sieci, jakie są następnie wybierane losowo do potwierdzania transakcji w kolejnych blokach. Obecnie najpopularniejszymi sposobami osiągania konsensusu są: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority (PoA).

* **Konsensus** (ang. consensus) – to automatyczny proces ustalania zgodności operacji w danej sieci blockchain pomiędzy jej użytkownikami, bez konieczności angażowania centralnej jednostki lub zaufanej strony trzeciej. Konsensus musi zostać każdorazowo osiągnięty, zanim blok zostanie dodany do łańcucha danych. Najbardziej znanym sposobem osiągania konsensusu jest Proof of Work (PoW).

ZASADY KONSENSUSU

	BEZPIECZEŃSTWO	WYDAJNOŚĆ I SKALOWANIE	KOSZTY	WYKORZYSTANIE
PoW	●●● wysokie w przypadku rozbudowanych sieci	●○○ niska wydajność i bardzo ograniczona skalowalność	●●● bardzo wysokie (głównie koszty energii elektrycznej)	sieci publiczne wykorzystujące kryptowaluty
PoS	●●○ niższe niż w PoW, zależne od dywersyfikacji tokenów (rośnie wraz z dywersyfikacją)	●●○ wyższa niż w PoW, jednak ograniczona od pewnego momentu rozwoju	●●○ niższe niż w PoW	sieci publiczne lub hybrydowe
DPoW	●●● wyższe niż w przypadku PoS	●●○ wyższa niż w PoW, jednak ograniczona od pewnego momentu rozwoju	●●○ niższe niż w PoW	sieci publiczne lub hybrydowe
PoA	●●● zależne od liczby jednostek nadzorujących sieć (rośnie wraz z liczbą tych jednostek)	●●● bardzo wysoka wydajność i skalowalność zależna od nakładów i sprzętu	●●○ niższe niż w PoW, zależne od liczby jednostek nadzorujących sieć	sieci prywatne

Źródło: Raport PWT pt. „Blockchain w Polsce. Możliwości i zastosowania".

●● **Wydatki na blockchain rosną w Europie z prędkością 80,2% rok do roku. Wg najnowszego raportu firmy badawczej IDC Stary Kontynent to drugi co do wielkości rynek dla tej technologii, prym wiodą USA, gdzie w blockchain inwestowane jest aż 40% całkowitych wydatków (globalna suma w 2018 r. przekroczyła 2 mld dol.).**

● **Proof of Work (PoW)** – najstarsza metoda, wykorzystana w sieci Bitcoin. W tym typie sieci wszystkie węzły mają możliwość zatwierdzenia kolejnego bloku danych, a prawdopodobieństwo dodania kolejnego bloku przez węzeł rośnie w momencie, gdy dostarcza on więcej mocy (określonej przez twórcę Bitcoina jako praca). W związku z tym cała sieć wymaga dostarczenia bardzo dużej ilości energii elektrycznej, potrzebnej do zasilania komputerów zamykających bloki danych. To przekłada się na wysokie koszty utrzymania tego typu sieci. Dodatkowo konieczność zatwierdzania każdego bloku przez wszystkich użytkowników znacząco spowalnia cały proces – sieć jest mniej efektywna od standardowych, scentralizowanych rozwiązań i oferuje mniejszą możliwość skalowania.

● **Proof of Stake (PoS)** – model konsensusu, w którym nagroda za zatwierdzenie bloku jest rozdysponowana zgodnie z liczbą posiadanych tokenów. W związku z tym sieć nie wymaga tak dużej mocy obliczeniowej jak w przypadku PoW, dzięki czemu system jest znacznie tańszy w utrzymaniu. Dodatkowo sieci wykorzystujące PoS są bardziej efektywne i oferują większą skalowalność (uwaga – od pewnego momentu możliwości skalowania tych sieci spadają, przede wszystkim z powodu rosnącej liczby węzłów zatwierdzających).

● **Delegated Proof of Stake (DPoS)** – modyfikacja PoS, polegająca na tym, że użytkownicy sieci głosują na jednostki, które w ich ocenie będą najlepiej zatwierdzały bloki danych. Głosowanie odbywa się przy zatwierdzaniu każdego kolejnego bloku i kończy się w momencie, gdy uda się osiągnąć satysfakcjonującą liczbę węzłów zatwierdzających. Dzięki takiej konstrukcji oraz mechanizmowi rankingowemu jednostki zatwierdzające bardziej dbają o jakość operacji dodawanych do bloku niż w standardowym PoS. Koszty działania są również znacząco niższe niż w PoW. Podobnie jednak jak PoS, również delegowana wersja tego konsensusu musi mierzyć się z problemem zbytnio rozbudowanej sieci jednostek potwierdzających operacje, ograniczających wydajność całej sieci. Dodatkowo sieci delegowane mogą być częściej wstrzymywane w wyniku braku wymaganej liczby wybranych węzłów zatwierdzających.

● **Proof of Authority (PoA)** – w ramach tego konsensusu istnieją z góry wyznaczone węzły nadzorujące, które stale zajmują się autoryzowaniem operacji. Tego typu sieci wymagają centralnego nadzoru, ponieważ w ich przypadku liczba węzłów powinna być dostosowywana do wielkości samej sieci (w przypadku pozostałych metod odbywa się to często w wyniku porozumienia uczestników sieci). Ważne jest przy tym bezpieczeństwo, które spada wraz ze zmniejszającą się liczbą węzłów oraz ich koncentracją (węzły skoncentrowane w jednym miejscu, np. wspólnej serwerowni, są bardziej narażone na skuteczny atak niż jednostki rozproszone). Dzięki temu jednak sieci te są bardzo wydajne oraz pozwalają na skalowanie do dużych rozmiarów.

50 000
TRANSAKCJI NA SEKUNDĘ

Obecne systemy finansowe rutynowo obsługują tysiące transakcji na sekundę. Na przykład system VISA przetwarza 2000 transakcji na sekundę, a w okresach szczytowego ruchu może obsłużyć ponad 50 000 transakcji na sekundę.

Publiczne sieci oparte na konsensusie Proof of Work mają znacznie niższą wydajność. Na przykład Bitcoin obsługuje około 6 transakcji na sekundę, a sieć Ethereum około 15 transakcji na sekundę. Jest to znacznie poniżej typowych wymagań biznesowych. Dlatego trwają intensywne prace, aby zwiększyć efektywność sieci blockchain. Takie działania nie mogą jednak wpływać na zmniejszenia wiarygodności tych sieci. Alternatywą jest zastosowanie sieci hybrydowych lub prywatnych. Na przykład platforma Hyperledger Fabric jest w stanie przetwarzać kilka tysięcy transakcji na sekundę. Drugim czynnikiem ograniczającym rozwój platformy blockchain jest wzrost wielkości bazy danych, który wynika z podstawowej cechy, jaką jest niezmienialność zapisów (bloki są ciągle dodawane do łańcucha i nie mogą być z niego usunięte). Tu również pomaga stosowanie sieci prywatnych lub hybrydowych, co ogranicza wolumen zapisywanych danych do tych niezbędnych dla konkretnego zastosowania biznesowego.

BUSINESS CONTINUITY i DISASTER RECOVERY W POLSKICH FIRMACH

Od kilku lat obserwujemy rosnący trend rozpowszechniania się złośliwego oprogramowania ransomware wśród różnej wielkości organizacji z różnych sektorów. Przedsiębiorstwa działające w Polsce są świadome tej sytuacji i jak pokazuje badanie firmy Veeam, powoli zwracają się ku rozwiązaniom umożliwiającym utrzymanie ciągłości biznesowej i odzyskiwania awaryjnego.

Sebastian Kuniszewski

Według badań FBI (Ransomware Prevention and Response for CISOs) od stycznia 2016 r. codziennie dochodziło do 4 tysięcy ataków z użyciem ransomware (wzrost o 300% w stosunku do 2015 r.). W 2017 r. byliśmy świadkami m.in. spektakularnych ataków wirusów WannaCry czy Petya oraz szybko rozprzestrzeniających się, sponsorowanych przez niektóre państwa wycieków i kampanii ransomware, wliczając w to ataki związane z wyborami. Niektórzy eksperci określili 2017 rokiem ransomware. Najnowszy (w momencie przygotowywania materiału) wariant tego typu zagrożenia o nazwie Saturn pojawił się w lutym 2018 r. i był oferowany za darmo jako usługa w znanym od około roku modelu **Ransomware-as-a-Service** (patrz ramka). Zaawansowane cyberzagrożenia na stałe wpisały się w wirtualną codzienność, a ataki komputerowe to intratny biznes – powinno to prowadzić do konstatacji, że tradycyjne metody ochrony danych nie są wystarczające i warto je uzupełnić o dodatkowe narzędzia.

Jakie inwestycje uważane są za priorytetowe w firmie?

Zapewnienie ciągłości biznesowej (DR) – 90%

Zabezpieczenie przed atakami hakerskimi i wirusami – **74,7%**

Ochrona przed wyciekiem danych (DLP) – **64,7%**

Migracja do chmury obliczeniowej – **23,8%**

Rozbudowa infrastruktury fizycznej w serwerowni/centrum danych – **36,1%**

Inne – **39,1%**

DEKLARACJE A ADAPTACJA TECHNOLOGII BC/DR

Przedsiębiorstwa działające w Polsce są świadome tej sytuacji. Badanie przeprowadzone przez firmę Veeam pokazało, że **aż 90% polskich organizacji deklaruje, że zapewnianie ciągłości biznesowej jest dla nich priorytetem**. Jednak sama świadomość potrzeby zagwarantowania ciągłości operacyjnej to pierwszy krok w kierunku wdrożenia odpowiednich rozwiązań.

Cieszy fakt, że polskie firmy doskonale zdają sobie sprawę z tego, że obecne zagrożenia mogą powodować poważne i kosztowne przestoje. Te zaś mogą zakłócać działalność organizacji do tego stopnia, że czasami powrócenie do punktu wyjścia może być trudne lub wręcz niemożliwe. Wciąż jednak pozostaje wiele do zrobienia, jeśli chodzi o budowanie przez przedsiębiorstwa bezpiecznej infrastruktury IT oraz utrzymanie ciągłości biznesowej na możliwie najwyższym poziomie. Polskie organizacje wciąż niechętnie wdrażają nowe technologie. Jednak takie czynniki, jak rosnące zapotrzebowanie na stałą dostępność danych czy wdrażanie rozwiązań chmurowych, mają wpływ na zwiększone zainteresowanie rozwiązaniami Business Continuity (BC) i Disaster Recovery (DR).

GŁOS MENEDŻERÓW I SPECJALISTÓW

Badanie „Rozwiązania Business Continuity / Disaster Recovery w polskich firmach" zostało przeprowadzone w celu zobrazowania tego, jak firmy i instytucje działające w Polsce podchodzą do kwestii gwarantowania ciągłości działania usług IT oraz rozwiązań do odzyskiwania awaryjnego. Sondaż przy użyciu ankiet na zlecenie Veeam zrealizowała agencja ITBC Communication. Grupę badawczą stanowiło 240 menedżerów i specjalistów ds. IT ze średnich i dużych przedsiębiorstw oraz instytucji, którzy uczestniczyli w konferencji VeeamON Tour Polska 2017. Ankietowani reprezentowali wszystkie kluczowe sektory gospodarki. Badanie zostało zrealizowane jesienią 2017 roku.

Jak często przeprowadzane są testy rozwiązania Disaster Recovery?

Co tydzień – **5,4%**

Co miesiąc – **14,9%**

Co kwartał – **16,9%**

Co pół roku – **23%**

Raz na rok lub rzadziej – 39,9%

USŁUGI DLA BIZNESU i... PRZESTĘPCÓW

DRaaS (Disaster Recovery as a Service) – mała popularność, duże korzyści

DRaaS wciąż nie jest popularną technologią w Polsce. Jeśli chodzi o wybór odpowiednich narzędzi do awaryjnego odzyskiwania danych oraz wybór określonej infrastruktury, firmy nadal skłaniają się ku bardziej tradycyjnej, wewnętrznej infrastrukturze informatycznej (37%). Technologie DRaaS, czyli odzyskiwanie awaryjne z wykorzystaniem rozwiązań chmurowych, są preferowane przez 29% respondentów. 24% firm preferuje rozwiązania DR bazujące na zapasowym centrum danych. Respondenci podzielili się również swoimi obawami dotyczącymi DRaaS. Największy opór budzą zależność od usługodawcy (32%) oraz spodziewane wysokie koszty usługi (23%). Na dalszym miejscu zgłaszane były obawy dotyczące utraty pełnej kontroli nad rozwiązaniem DR (13%). Są to prawdopodobnie główne przyczyny, z powodu których DRaaS nie jest jeszcze w Polsce popularnym rozwiązaniem.

Równocześnie widoczna jest też pozytywna zmiana w podejściu polskich organizacji do technologii chmurowych, a **kolejne firmy dostrzegają korzyści, jakie przynosi DRaaS**. Przede wszystkim wymieniane są: eliminacja potrzeby tworzenia zapasowego centrum danych (25%), szybkość przełączania na zapasową infrastrukturę (21%), oszczędność czasu (17%), elastyczny model płatności (15%), ekonomiczność (13%) oraz brak konieczności samodzielnego zarządzania narzędziem DR (9%).

W jaki sposób strategia Disaster Recovery może być realizowana w firmie?

W oparciu o wewnętrzną infrastrukturę firmy – 37,1%

W oparciu o ośrodek zapasowy (Disaster Recovery Center) – **24,3%**

W oparciu o chmurę/usługi Disaster Recovery as a Service – **26,6%**

Nie wiem – **10%**

RaaS – Ransomware-as-a-Service – minimum pracy, maksimum zysku

Ransomware dostępny w modelu usługowym pozwala wynająć od cyberprzestępców określone zagrożenie i zarabiać na infekowaniu komputerów w sieci. Cena za wejście do przestępczego procederu i używanie gotowego rozwiązania jest niska – procent od udziałów w haraczach, który autorzy wirusa odliczają od wpłat wpływających na konto cyberprzestępcy (np. w przypadku Satana, pierwszego ransomware w modelu RaaS wykrytego w lutym 2017 r., było to 30%). Prowizję można zmniejszyć, infekując coraz większą liczbę komputerów, do czego motywują „usługodawcy". Po rejestracji i zalogowaniu na stronie usługi użytkownik otrzymuje dostęp do konsoli afiliacyjnej i krok po kroku prowadzony jest podczas tworzenia własnej wersji narzędzia szyfrującego. Zazwyczaj dostępna jest też szczegółowa instrukcja użytkowania narzędzia, a korzystanie z usługi może usprawniać np. system powiadomień o nowych opcjach kreatora złośliwego kodu. Personalizując wirusa, można m.in. określić wysokość okupu, liczbę dni, po których haracz wzrasta, oraz mnożnik jego wzrostu. Dostawcy RaaS przygotowują również porady, jak promować i rozprzestrzeniać „swojego" wirusa czy implementować złośliwy kod np. w makrach dokumentów Office (zaszywając zainfekowane ramki w fałszywych dokumentach, wysyłanych podczas kampanii spamowych). Oczywiście użytkownik może też przetłumaczyć wyświetlane informacje na inne języki, aby – cytując twórców jednej z usług – „ofiary lepiej rozumiały, co się dzieje".

UTRZYMANIE DOSTĘPNOŚCI DANYCH TO WYZWANIE

ANDRZEJ NIZIOŁEK
starszy menedżer regionalny Veeam Software

Gwałtowny wzrost ilości informacji i cyberzagrożeń sprawia, że utrzymanie dostępności danych nie jest prostym procesem – wymaga czasu, uwagi, zaangażowania i konsekwencji. Wdrożenie rozwiązania dostępności – choć jest koniecznością dla każdej organizacji – to pierwszy krok na drodze do zapewnienia ochrony danych i infrastruktury w obliczu zmieniającego się krajobrazu zagrożeń. Nie można zapobiec przestojom bez odpowiedniej polityki tworzenia kopii zapasowych. Oprócz faktu, że istnieją jeszcze firmy, które nie wdrożyły żadnej technologii dostępności, widzimy niepokojące zjawisko zaniechania przez firmy testowania tego typu rozwiązań. Często też przedsiębiorstwa nie mają zdefiniowanego planu odzyskiwania danych po awarii. Sama inwestycja w nowe technologie nie zapewni ochrony – konieczne jest regularne testowanie posiadanych rozwiązań.

WNIOSKI Z BADANIA

WIELE FIRM BEZ WDROŻONYCH TECHNOLOGII DOSTĘPNOŚCI

Prawie jedna trzecia polskich firm nie wdrożyła jeszcze rozwiązań z zakresu dostępności danych. Przedsiębiorstwa deklarują, że uważają ochronę przed atakami cybernetycznymi, naruszeniami i wyciekami danych za bardzo ważną, ale z badania wynika, że **nie dysponują technologiami dostępności i awaryjnego odzyskiwania danych**.

INCYDENTY NARUSZENIA BEZPIECZEŃSTWA IT W 2017 r.

Ryzyko naruszeń bezpieczeństwa informatycznego wzrasta wraz z ilością przetwarzanych i udostępnianych danych oraz urządzeń podłączonych do sieci. Oba czynniki są warunkowane postępującą wśród polskich organizacji cyfrową transformacją biznesu. **Tylko 8% ankietowanych przedsiębiorstw nie doświadczyło w ubiegłym roku żadnych incydentów związanych z bezpieczeństwem lub dostępnością**. 12% firm padło ofiarą ataku z wykorzystaniem ransomware lub innego rodzaju złośliwego oprogramowania, co spowodowało nieplanowane przestoje.

ORGANIZACJE TWORZĄ PLANY DZIAŁANIA NA WYPADEK ZAISTNIENIA INCYDENTU IT

Choć niemal wszystkie badane firmy deklarowały, że stała dostępność i ciągłość biznesu jest dla nich kluczowa i są świadome skali zagrożeń, to jednak wiele z nich **nie jest w żaden sposób przygotowana na poważne incydenty informatyczne, które zagrażają bezpieczeństwu ich danych biznesowych**. Według badania Veeam realizacja planów odzyskiwania awaryjnego została zadeklarowana przez 63% respondentów. Jest to obiecujący wynik, choć nadal wiele pozostaje do zrobienia.

FIRMY NIE TESTUJĄ WDROŻONYCH TECHNOLOGII DISASTER RECOVERY

W odniesieniu do firm, które wdrożyły rozwiązania w zakresie dostępności, istnieją realne obawy związane z prawidłowym użytkowaniem tych technologii. Większość organizacji (60%) stosujących rozwiązania BC/DR nie przeprowadza terminowych testów dostępności lub nie tworzy odpowiednich polityk w celu ochrony przed zagrożeniami. **40% z nich zaniedbuje również regularne testy technologii, poprzestając jedynie na przeświadczeniu, że jednorazowa inwestycja jest wystarczającą gwarancją utrzymania bezpieczeństwa**.

DISASTER RECOVERY CENTER – RODO I CIĄGŁOŚĆ DZIAŁANIA

TOMASZ ANDRZEJCZUK
analityk Centrum Danych Asseco Data Systems

Po wejściu w życie rodo zwiększy się popyt na profesjonalne systemy, takie jak DLP (Data Loss Prevention) i DRC (Disaster Recovery Center). Pozwalają one zarządzać wrażliwymi danymi, które znajdują się w różnych środowiskach, tak by były one chronione przed przypadkowym lub zamierzonym wyciekiem (DLP) oraz zapewniają ciągłość działania organizacji w przypadku wystąpienia awarii (DRC). Podstawą zastosowania jest fakt, że zapasowe, zewnętrzne centrum danych znajduje się w odległej lokalizacji i jest gotowe przejąć rolę ośrodka podstawowego w ustalonym czasie – tak aby firma mogła możliwie płynnie prowadzić swoją działalność. Klienci nie muszą martwić się o bezpieczeństwo, bieżące aktualizacje systemów, własne serwery, dostawców energii, internetu czy wyposażenie techniczne pomieszczeń i inne aspekty związane z posiadaniem własnej infrastruktury.

5 WIODĄCYCH TRENDÓW W **OBSZARZE IoT**

Ostatnie lata to masowy wzrost zainteresowania i oczekiwań w stosunku do technologii IoT. Dotychczas jednak większość rozwiązań stanowią zamknięte systemy o ograniczonych możliwościach współpracy pomiędzy sobą. Według globalnej grupy ekspertów EY z Centrum Kompetencyjnego Internetu Rzeczy w 2018 r. wiodącymi trendami w obszarze IoT będą: powstawanie nowych modeli biznesowych bazujących na cyfryzacji, monetyzacja danych IoT, integracja pojedynczych technologii we wspólne rozwiązania oraz rozwój architektury przetwarzania peryferyjnego, czyli tzw. network edge processing.

Sebastian Kuniszewski

MONETYZACJA IoT – WYSPY AUTOMATYZACJI I EKOSYSTEMY NOWYCH USŁUG

Sposoby wykorzystywania możliwości technicznych rozwiązań działających w ramach Internetu rzeczy obecnie są wciąż bardzo tradycyjne i koncentrują się na poprawie efektywności procesów oraz optymalnego wykorzystania środków trwałych. Obrazowo można porównać to do tworzenia swojego rodzaju wysp automatyzacji, a całe zjawisko przypomina początkowe lata wdrażania komputerów w przedsiębiorstwach. Jednak coraz większa liczba osób zarządzających firmami zaczyna dostrzegać przełomowy charakter nowej technologii jako narzędzia pozwalającego na zmianę modeli biznesowych i operacyjnych przedsiębiorstw. IoT umożliwia bowiem kontrolę produktu nie tylko w procesie produkcyjnym, ale także w drodze do użytkownika końcowego i w trakcie użytkowania. Podłączenie do sieci różnego rodzaju produktów pozwala na budowę nowych usług, bazujących na danych pochodzących z komponentów IoT zintegrowanych z ich fizycznymi odpowiednikami.

Komentarz A.P.:
- Kiedy menedżerowie uświadomią sobie potencjał kreowania wartości jaki mają systemy IoT, poszukają nowych obszarów dostarczania klientom lepszej jakości usług i zmieniających obecne procesy biznesowe. W 2018 roku oczekujemy wielu pilotażowych wdrożeń rozwiązań IoT oraz akwizycji start-upów, które w swoim portfolio mają już gotowe produkty. Konsekwencją tego wzrostu aktywności będą prace nad transformacją obecnych modeli biznesowych i operacyjnych, tak aby dostosować je do nowych możliwości oferowanych przez technologie IoT oraz rosnącą integrację tradycyjnych produktów z sensorami IoT.

STANDARYZACJA TRANSMISJI, KONTROLA NAD ŁĄCZNOŚCIĄ IoT

Głównym ograniczeniem dla interoperacyjności IoT jest niejednolita komunikacja. Poszczególni dostawcy promują różne rozwiązania transmisyjne dla własnych rozwiązań, a efektem jest stan obecny – istnienie wielu zamkniętych systemów o ograniczonych możliwościach współpracy i wymiany danych. Eksperci EY uważają, że w 2018 roku na znaczącą zmianę sytuacji wpłyną prace nad standardem sieci komórkowej 5G. W szczególności oczekuje się wirtualizacji sieci o różnych charakterystykach, dostosowanych do indywidualnych wymogów funkcjonalnych rozwiązań oraz możliwości transmisyjnych w różnych warunkach, przy wykorzystaniu szerokiego spektrum częstotliwości. O ile szerokie komercyjne wdrożenia sieci 5G nastąpią nie wcześniej niż w 2020 roku, to formalne standardy powinny pojawić się już w tym roku, podobnie jak pilotażowe wdrożenia w niektórych krajach azjatyckich. Z pewnością będzie to silny impuls do dalszych prac rozwojowych nad nowymi rozwiązaniami IoT.

Komentarz A.P.:
- IoT nie może się rozwijać bez efektywnej i rozsądnej kosztowo sieci bezprzewodowej, interoperacyjności oraz wspólnych standardów. Jesteśmy przekonani, że 5G może mieć przełomowy wpływ na sposób, w jaki przyszłe ekosystemy IoT będą projektowane, zwłaszcza jeśli chodzi o ich skalowalność, opóźnienia, niezawodność, bezpieczeństwo oraz poziom indywidualnej kontroli parametrów przyłączeniowych.

POPULARYZACJA PRZETWARZANIA PERYFERYJNEGO

Od wielu lat w świecie IoT ścierają się dwie główne koncepcje dotyczące miejsca przetwarzania gromadzonych danych w czujnikach w użyteczne informacje. Pierwsza zakłada wysyłanie surowych danych do obróbki w chmurze, druga opiera się na tym, że czujniki (najczęściej powiązane ze sobą) mają własny procesor i wysyłają dalej już przetworzoną informację. Jest to tzw. przetwarzanie peryferyjne (processing on the edge), w ramach którego zamiast wysyłać np. ciąg parametrów z samosterującego samochodu, wysyła się tylko odległość od najbliższego obiektu, albo położenie geograficzne, a pozostałe dane obrabiane są przez lokalne urządzenia. Paradoksalnie trend dążący do popularyzacji przetwarzania peryferyjnego i przesyłania jedynie użytecznej informacji był dotychczas skutecznie spowalniany przez spadające ceny komunikacji i coraz większą przepustowość udostępnianych łączy sieciowych. Jednak postępująca miniaturyzacja i spadek kosztów produkcji urządzeń końcowych IoT powinien przełożyć się na wzrost popularności przetwarzania peryferyjnego w nowych rozwiązaniach.

ALEKSANDER PONIEWIERSKI,
Global IoT Leader, EY
Ekspert ds. cyberbezpieczeństwa oraz infrastruktury krytycznej. Skupia się na rozwoju strategii, projektowaniu, wdrażaniu i optymalizacji procesów biznesowych oraz zagadnieniach bezpieczeństwa i ochrony IoT dla globalnych klientów, zarówno w branży konsumenckiej, jak i przemysłowej. Doktor nauk ekonomicznych Uniwersytetu Ekonomicznego w Poznaniu. Uczestnik prestiżowych programów organizowanych przez Harvard Business School oraz Carnegie Mellon University.

50%

niemal tyle firm oczekuje oporu ze strony pracowników wobec wprowadzenia rozwiązania IoT. Jednocześnie większość z nich nie ma pomysłu na rozwiązanie tego problemu. Jedynie 21% z nich przygotowało plan, jak na problem zareagować.

OD CYBERBEZPIECZEŃSTWA DO CYBERODPORNOŚCI

Eksperci EY z Centrum Kompetencyjnego IoT podkreślają, że zagrożenia cyberprzestrzeni i regulacje dotyczące m.in. ochrony prywatności są istotną barierę dla szerokiego wykorzystania rozwiązań IoT. Przedsiębiorstwa coraz częściej zdają sobie sprawę z tego, że metody skuteczne w przypadku zabezpieczania scentralizowanych systemów IT są nieadekwatne dla rozproszonych systemów IoT. Dlatego w kolejnych latach oczekiwany jest raczej zwrot w kierunku podwyższania odporności rozproszonych systemów jako całości, a nie, jak dotychczas, koncentrowanie się na zabezpieczaniu indywidualnych komponentów.

Komentarz A.P.:
- Różne wymagania dotyczące współpracy urządzeń końcowych z infrastrukturą transmisyjną (np. w zakresie przepustowości, opóźnień czy efektywności energetycznej) wymusiły odejście od filozofii „one-fits-for-all" na rzecz nowych specjalistycznych rozwiązań. Równolegle regulacje dotyczące ochrony prywatności, obowiązujące w szczególności w Europie, skutkują odchodzeniem od przesyłania nieprzetworzonych, niezabezpieczonych danych do publicznych chmur. W efekcie oczekiwać możemy renesansu rozwiązań bazujących na przetwarzaniu peryferyjnym.

- Rozwiązania IoT wymagają jednoczesnego spełnienia warunku bezpieczeństwa użytkowania, ochrony prywatności, niezawodności oraz odporności. Tego nie da się osiągnąć, zabezpieczając poszczególne elementy środowiska mającego wiele celów. Konieczna jest zmiana podejścia. Zamiast ograniczać się do ochrony przed niepowołaną ingerencją, należy projektować całe systemy z nadrzędną myślą o zapewnieniu ich odporności (resilience-by-design) na różnego typu zagrożenia. Pozwoli to na zapewnienie ochrony gromadzonych, przetwarzanych i transmitowanych danych, adekwatnie do ich wykorzystania we wsparciu funkcjonowania istniejącej infrastruktury, procesów biznesowych oraz wymogów regulacyjnych.

INTEGRACJA ROZPROSZONYCH TECHNOLOGII

Dotychczas rozwiązania bazujące na IoT, blockchain (Distributed Ledger Technologies – DLT), algorytmach samouczących się i sztucznej inteligencji (Artificial Intelligence – AI) czy automatyzacji procesów biznesowych (Robotic Proces Automation, RPA) wdrażane były niezależnie. Jednak obserwowane trendy zapewnienia ich pełnej konwergencji i interoperacyjności sprawiają, że w najbliższej przyszłości ich integracja będzie traktowana po prostu jako etap transformacji cyfrowej. Eksperci EY oczekują pojawienia się w 2018 roku w pełni zintegrowanych systemów wykorzystujących wymienione technologie do budowy rozwiązań klasy inteligentnej automatyzacji procesów (Intelligent Process Automation – IPA).

Komentarz A.P.:
- Z biznesowego punktu widzenia przełomowe technologie uzupełniają już istniejące systemy i pełnią unikalną rolę w różnych obszarach organizacji. Na początku menedżerowie są zafascynowani możliwościami pojedynczych technologii. Z czasem oczekiwać będą zintegrowanego podejścia i optymalizacji zwrotu z inwestycji.

70%

firm jest zdania, że czynnikiem, który najskuteczniej stymuluje inwestycje w IoT, jest poprawa doświadczeń klientów. W przyszłości najważniejszymi czynnikami prawdopodobnie będą: zwiększanie dochodu (53% badanych) oraz wejście na nowe rynki (51%).

ŹRÓDŁO: ZEBRA TECHNOLOGIES

OPORNI NA CYFROWĄ TRANSFORMACJĘ

POLSKIE FIRMY CYFROWO UPOŚLEDZONE

W ubiegłym roku zaledwie 6% polskich firm analizowało duże zbiory informacji – wynika z danych Eurostatu. Daje nam to przedostatnie miejsce w unijnym rankingu, przed Cyprem. Liderami pod względem digitalizacji i korzystania z big data są Malta i Holandia. W tych krajach niemal już co piąta firma analizuje cyfrowe informacje.

Jerzy Michalczyk

W ubiegłym roku zaledwie co trzecia firma działająca w UE, zatrudniająca co najmniej 10 osób, posiadała stronę internetową. Choć znacznie lepiej wyglądają wskaźniki wykorzystania mediów społecznościowych w działaniach biznesowych – przyznaje się do tego już połowa firm – to ten wyjątek tylko potwierdza regułę: cyfryzacja to pięta achillesowa wielu przedsiębiorstw. Nie tylko polskich. Najlepiej ilustrują to dane na temat wykorzystania big data.

Polska daleko w tyle

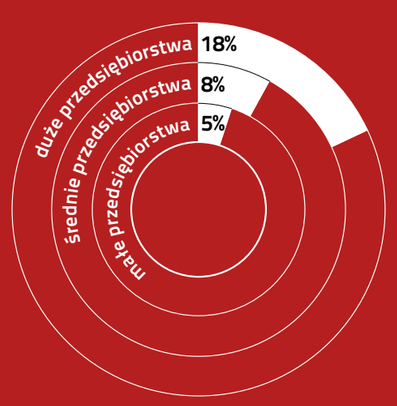
Jak wynika z unijnych danych, w UE tylko 10% firm analizuje duże zbiory informacji o klientach, rynku czy konkurencji. To oczywiście średnia, są kraje, gdzie z danych korzysta się znacznie częściej, niemniej te liczby pokazują, że big data znajduje się na podobnym etapie rozwoju jak kilka lat temu chmura obliczeniowa. „Biznes do cloud computingu podchodził na początku bardzo ostrożnie; dopiero gdy zobaczył efekty wdrożenia chmury, znacznie szybciej zaczął adaptować tę technologię. Podobnie będzie z big data" – zwraca uwagę Piotr Prajsnar, CEO Cloud Technologies, spółki zarządzającej jedną z największych na świecie hurtowni danych.

Ten wzrost już widać, co dobrze ilustrują dane spółki, która jeszcze w II kwartale ubiegłego roku z usług opartych na big data wygenerowała 12 mln zł, a rok później już 16,7 mln zł. Na razie w unijnym rankingu Polska wypada jednak bardzo słabo. Tylko 6% polskich firm korzysta z analityki big data, co daje nam w ogólnej klasyfikacji 24., przedostatnie miejsce, przed Cyprem. Lepiej wypadają od nas m.in. Rumunia, Czechy, Słowacja czy Bułgaria. Podium zajmują Malta, Holandia i Belgia, kolejne pozycje zajęły takie państwa jak Finlandia, Wielka Brytania czy Estonia.

Duże firmy radzą sobie lepiej

Dystans, jaki dzieli nas od dobrze zinformatyzowanych, ucyfrowionych państw, dobrze pokazuje nasycenie rozwiązaniami big data w dużych firmach. W Polsce z analityki danych korzysta 5% małych, 8% średnich i 18% dużych, zatrudniających powyżej 250 osób

FIRMY W POLSCE KORZYSTAJĄCE Z ANALIZY BIG DATA



1% FIRM W POLSCE KORZYSTA Z ZEWNĘTRZNYCH ŹRÓDEŁ DANYCH, ŚREDNIA W EUROPIE TO 25%!

46% PRZEDSIĘBIORSTW PRZYZNAJE SIĘ, ŻE ANALIZUJĄ DANE GEOLOKALIZACYJNE Z URZĄDZEŃ PRZENOŚNYCH!

przedsiębiorstw. Dla porównania, na Malcie takich firm jest 42%, w Danii i Finlandii 40%, a u naszych południowych sąsiadów – Słowaków i Czechów – odpowiednio 24% i 22%.

Najczęściej firmy analizują dane geolokalizacyjne z urządzeń przenośnych, do czego przyznaje się aż 46% przedsiębiorstw, a także dane generowane w mediach społecznościowych (45% wskazań). Co trzecia firma analizuje dane własne pozyskane ze smart urządzeń i sensorów. Dla porównania, w Polsce dane z urządzeń smart pozyskuje 10% firm, tyle samo wykorzystuje informacje geolokalizacyjne. Co ciekawe, dane pozyskane z mediów społecznościowych analizuje zaledwie 5% firm. – Najczęściej sięga po nie branża marketingowa, a w szczególności e-commerce, bo mają one największą świadomość korzyści. Dzięki analizie informacji z różnych źródeł można bardzo dobrze poznać zainteresowania i potrzeby klienta i tym samym znacząco zwiększyć skuteczność kampanii reklamowych i sprzedaż produktu. Widać także rosnące zainteresowanie analizą danych ze strony instytucji finansowych oraz firm działających w segmencie B2C, które wzbogacają nimi swoje systemy CRM.

Przyszłość analityki big data

Firma analityczna IDC szacuje, że rynek big data rośnie dziś w tempie 11,7% rok do roku i w 2020 r. osiągnie wartość 203 miliardów dolarów. Jaka część tego tortu przypadnie Polsce? Jak wynika z unijnych danych, proces digitalizacji polskich przedsiębiorstw postępuje dużo wolniej, niż ma to miejsce w większości innych państw UE. To o tyle ciekawe, że autorzy rankingu „Digital Economy and Society Index 2017" (w którym Polska zajmuje odległe, 23. miejsce), zwracają uwagę na to, że poczyniliśmy postępy m.in. w obszarze cyfryzacji społeczeństwa, wdrażania szybkich połączeń internetowych czy korzystania z mobilnych usług szerokopasmowych. Jednak wprowadzanie technologii cyfrowych przez przedsiębiorstwa idzie nam wyjątkowo opornie, podczas gdy unijny wskaźnik w tym obszarze rośnie nieprzerwanie od 2014 r., to w Polsce od ubiegłego roku utrzymuje się na niemal tym samym poziomie. Oznacza to, że dystans dzielący nas od liderów systematycznie się powiększa.

W tej sytuacji warto zastanowić się nad skorzystaniem z usług Data as a Service w tym modelu nie trzeba inwestować we własne rozwiązania. Jak wynika z danych Eurostatu, z zewnętrznych źródeł danych korzysta jedna czwarta firm. W Polsce to zaledwie 1%.

> **PIOTR ROJEK, dyrektor zarządzający DSR, firmy dostarczającej zaawansowane rozwiązania dla produkcji**
> Statystyki wykorzystania chmury pokazują tylko wycinek rzeczywistości. Rynek chmury w Polsce, podobnie jak i w rozwiniętych krajach Europy, rośnie bardzo szybko, bez większego problemu można zwiększać sprzedaż o kilkadziesiąt procent każdego roku. Statystyki zaniżają jednak małe firmy, które do cloud computingu odnoszą się z większą rezerwą niż największe przedsiębiorstwa. Wynika to z wielu powodów: niewystarczającej świadomości potrzeb i korzyści, obaw, a także dużej rezerwy do relatywnie nowych rozwiązań.

POLSKA DALEKO OD CHMURY – ODLEGŁE MIEJSCE W UE!

Z danych Eurostatu wynika również, że podobnie jak w przypadku analizy dużych zbiorów danych, polskie przedsiębiorstwa wciąż rzadko korzystają z chmury obliczeniowej. Nasz kraj został sklasyfikowany na 28. miejscu unijnego rankingu! W ciągu dwóch lat awansowaliśmy zaledwie o jedno miejsce.

W Finlandii, będącej liderem zestawienia Eurostatu, z chmury obliczeniowej korzysta 57% rzedsiębiorstw. Na drugim biegunie sklasyfikowano Rumunię, Bułgarię oraz Macedonię, gdzie zaledwie 6% przedsiębiorstw przyznaje się do wykorzystywania chmury. Niestety, Polska znajduje się zaraz przed nimi, z 8% odsetkiem firm korzystających z cloud computingu. Wyprzedzają nas nie tylko rozwinięte zachodnie kraje, takie jak Dania (42%), Holandia czy Wielka Brytania (35%), ale także nasi południowi sąsiedzi: Czechy i Słowacja (po 18%). W ciągu dwóch lat (2014–2016) liczba przedsiębiorstw korzystających z chmury wzrosła w Polsce zaledwie o 1%.

W segmencie największych firm, zatrudniających powyżej 250 pracowników, wypadamy lepiej. Zajmujemy wciąż dalekie, bo 25. miejsce, ale z 31% firm korzystających z cloud computingu wyprzedzamy m.in. Czechy i Słowację (odpowiednio 30 oraz 28% wskazań). Liderem w segmencie dużych firm wciąż jest Finlandia, gdzie aż 87% firm używa chmury. Dla porównania, w sektorze małych firm Polska znalazła się na końcu rankingu z zaledwie 6% wynikiem – ramię w ramię z Bułgarią i Macedonią.

EUROPA UCIEKA

Niestety, mimo całkiem niezłych wyników w segmencie największych firm systematycznie powiększa się dystans, jaki dzieli nas od dobrze zinformatyzowanych zachodnich krajów. Dla przykładu w Szwecji w ciągu 2 lat liczba firm korzystających z chmury zwiększyła się z 39 do 48%. W Wielkiej Brytanii z 24 do 35%, a w bliskich nam geograficznie Czechach z 13 do 19%. W Polsce w tym czasie odnotowaliśmy wzrost z 6 do 8%.

Jeszcze dobitniej widać różnice, kiedy analizuje się sektor największych firm. W Finlandii liczba przedsiębiorstw zatrudniających powyżej 250 pracowników i korzystających z chmury wzrosła z 69 do 87%, w Belgii z 44 do 64%, w Polsce w tym samym czasie z 19 do 31%. Dobrą informacją jest to, że rośniemy tutaj szybciej niż Czechy czy Słowacja.

PROGNOZY – NIECO LEPSZE

Według firmy doradczej IDC sprzedaż rozwiązań chmurowych w latach 2017–2021 będzie rosła w Polsce w tempie ponad 18%. W ubiegłym roku w Polsce firmy sprzedały usługi chmurowe za kwotę 175 mln dolarów. W tym roku wartość rynku przekroczy próg 200 mln dolarów, ale w 2019 r. zbliży się już do poziomu 300 mln dolarów.

Jak wynika z opublikowanego przez firmę Domo raportu „Data Never Sleeps 5.0", w ciągu minuty internauci publikują ponad 46 tys. zdjęć na Instagramie, korzystają z wyszukiwarki Google ponad 3,5 mln razy i umieszczają ponad 74 tys. postów w mikroblogowym serwisie Tumblr. To kopalnia wartościowych informacji. Jednak na razie wykorzystywana rzadko. Jak wynika z unijnych danych, w UE tylko 10% firm analizuje duże zbiory informacji o klientach, rynku czy konkurencji.

QUALCOMM SNAPDRAGON 845

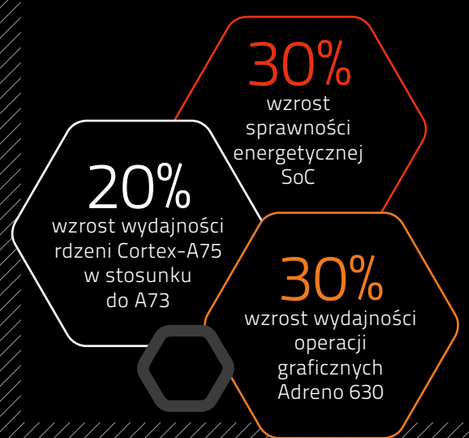
Duże zmiany w architekturze nowych procesorów Qualcomma – Snapdragonów 845 – przyniosą poprawę wydajności przetwarzania grafiki o ponad 30% i również 30-procentowe zmniejszenie zużycia energii w stosunku do modeli poprzedniej generacji (Snapdragon 835), a także 2,5-krotnie większą przepustowość wyjścia wideo, co pozwoli na obsługę rozdzielczości 2Kx2K z częstotliwością 120 Hz. Czego jeszcze możemy oczekiwać po nowych mobilnych CPU?

Jerzy Michalczyk

W grudniu ubiegłego roku firma Qualcomm przedstawiła specyfikację Snapdragona 845, następcy ubiegłorocznego topowego modelu Snapdragon 835. Nowy model to nie tylko zmiana cyferki w numeracji procesora, ale przede wszystkim duży krok naprzód w rozwoju technologii systemów SoC (System on Chip). 845 jest pierwszym modelem, w którym zastosowano zupełnie nową architekturę klastrową o nazwie DynamIQ, pozwalającą na znacznie większą elastyczność w projektowaniu układów scalonych w stosunku do używanej do tej pory w procesorach mobilnych topologii big.LITTLE. Mówiąc w skrócie, DynamIQ umożliwia stosowanie rdzeni różnego typu ze wspólną pamięcią cache w obrębie jednego klastra, w przeciwieństwie do konieczności zastosowania kilku (co najmniej dwóch) różnych klastrów w celu użycia rdzeni o różnych parametrach wydajnościowych i energetycznych. To najważniejsza zmiana, jaka zaszła w konsumenckich rozwiązaniach SoC w ciągu ostatnich pięciu lat. Więcej szczegółów na ten temat podajemy w dalszej części artykułu.

W najnowszym Snapdragonie znajdą się cztery wysokowydajne rdzenie Kryo 385, zgodne z architekturą Cortex-A75 i taktowane zegarem o częstotliwości do 2,8 GHz, oraz cztery rdzenie ekonomiczne Cortex A-55 taktowane zegarem o częstotliwości do 1,8 GHz. Wszystkie rdzenie zostaną rozmieszczone w obrębie pojedynczego klastra i będą mogły być swobodnie przełączane w zależności od zapotrzebowania na moc obliczeniową. Rdzeniom towarzyszyć będzie nowa pamięć podręczna trzeciego poziomu o pojemności 2 MB, a także pamięć cache systemowa o pojemności 3 MB. Dzięki tym zabiegom wydajność CPU nowego SoC powinna być o ok. 25% lepsza w porównaniu z poprzednikiem.

Obok samego CPU w ramach chipa SoC znajdzie się też nowy układ GPU o nazwie Adreno 630, nowy procesor obrazu Spectra 280, nowy DSP Hexagon 685 oraz modem Snapdragon X20 (LTE). Nowy model CPU ma być produkowany w ulepszonym 10-nanometrowym procesie litograficznym FinFET LPP (Low Power Plus) i według Qualcomma przy rejestrowaniu wideo, w grach czy z aplikacjami XR ma pobierać o jedną trzecią energii mniej niż Snapdragon 835.



DYNAMIQ – NOWA ARCHITEKTURA KLASTRÓW CPU

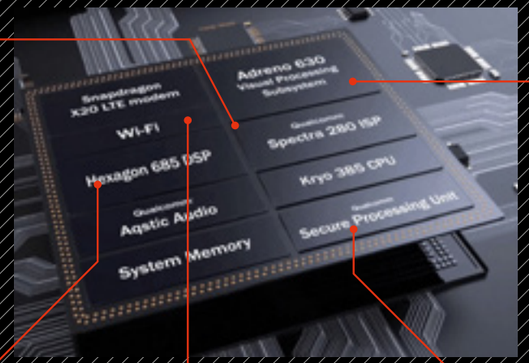
DynamIQ to następca wprowadzonej w 2012 roku technologii big.LITTLE, która pozwalała na zamienne stosowanie klastrów złożonych z maksymalnie czterech rdzeni, w zależności od bieżącego zapotrzebowania na moc obliczeniową. Klaster złożony z rdzeni bardziej wydajnych i taktowanych wyższą częstotliwością był włączany w razie konieczności dostarczenia większej wydajności, a klaster złożony z wolniejszych rdzeni cechował się niskim poborem prądu i był wykorzystywany w celu oszczędzania energii i wydłużenia czasu pracy baterii. Twórca technologii, firma ARM, już w 2013 roku rozpoczął prace nad rozszerzeniem tej technologii, które zapewniłoby większą elastyczność, skalowalność i wyższą wydajność.

Tak powstała architektura DynamIQ big.LITTLE również pozwalająca na grupowanie w ramach klastrów wielu rdzeni CPU oraz łączenie ich z innymi układami i elementami systemu. Jednakże w przypadku technologii big.LITTLE rdzenie o różnej wydajności muszą znajdować się w odrębnych klastrach, natomiast DynamIQ pozwala na grupowanie w jednym klastrze rdzeni o różnej wydajności. **Ponadto teraz można zgrupować w nim do ośmiu rdzeni, a samych klastrów może być nawet 32. Całkowita liczba rdzeni może więc wynieść 256, a nawet 1000 przy zastosowaniu magistrali CCIX umożliwiającej pracę wieloprocesorową**.

Rdzenie wewnątrz klastra są grupowane w tzw. domeny o tym samym napięciu zasilania i tej samej częstotliwości taktowania. W każdym klastrze można utworzyć do ośmiu takich domen. Co więcej, każdy rdzeń może zostać indywidualnie włączony lub wyłączony. Teoretycznie możliwe jest również przypisanie indywidualnych parametrów pracy każdemu rdzeniowi pracującemu w ramach klastra.

AUTOPSJA > Procesory mobilne

QUALCOMM SPECTRA 280 ISP
Nowy procesor ISP umożliwi m.in. przetwarzanie 16-megapikselowych obrazów z szybkością 60 klatek na sekundę, nagrywanie wideo w rozdzielczości 4K z HDR @ 60 FPS, rejestrację 10-bitowego koloru, międzyramkową redukcję szumów oraz tryb slow motion 720p @ 480 FPS. Ponadto umożliwi tworzenie obrazu 3D fotografowanych obiektów bez konieczności użycia oświetlenia laserowego czy czujników podczerwieni. Nowy układ może przetwarzać obraz z dwóch matryc aparatów cyfrowych i na tej podstawie odwzorować obserwowane obiekty w postaci obrazu trójwymiarowego.



ADRENO 630 VISUAL PROCESSING SUBSYSTEM
Najnowszy SoC zostanie wyposażony w nowy procesor graficzny Adreno 630 integrujący w sobie funkcje GPU, VPU oraz DPU. Niestety, producent nie udostępnił zbyt wielu szczegółów technicznych na ten temat. Z doniesień medialnych wiadomo jednak, ze ma on oferować o 20% lepszą sprawność energetyczną od swojego poprzednika, a wzrost wydajności powinien wynieść 30% przy 2,5-krotnym wzroście przepustowości przetwarzania danych.

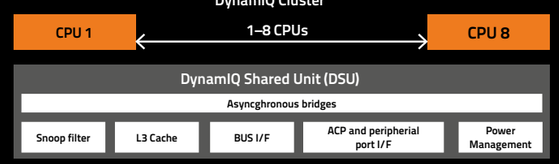
HEXAGON 685 DSP
Nowy procesor sygnałowy znajdzie zastosowanie w przetwarzaniu obrazu, dźwięku i do zadań związanych z rozszerzoną rzeczywistością oraz sztuczną inteligencją. Qualcom zapowiada, że w stosunku do układu 632 zastosowanego w Snapdragonach 835 możliwości nowego układu w zakresie obsługi AI wzrosną trzykrotnie.

X20 MODEM ORAZ WI-FI
Modem Snapdragon X20 wspiera standard LTE Cat. 18 i może agregować pasmo z pięciu kanałów 20 MHz, pozwalając na pobieranie danych z maksymalną prędkością 1,2 Gbit/s, co oznacza kolejny krok na drodze do standardu 5G. Wysyłanie danych możliwe jest z prędkością do 150 Mbit/s.

Ponadto procesor zapewni obsługę Wi-Fi w standardzie 802.11ac na 2,4, 5 i 60 GHz Bluetooth w wersji 5.0. Za obsługę dźwięku odpowiadać ma kodek audio Qualcomma WCD934x. PCM obsługiwane jest do 384 kHz/32-bit. W przypadku nagrywania dźwięku maksymalna jakość to 192 kHz/24 bit.

QUALCOMM SECURE PROCESSING UNIT (SPU)
W celu zapewnienia większego bezpieczeństwa Snapdragon 845 zawiera odrębną jednostkę SPU (Secure Processing Unit), której zadaniem jest bezpieczne przechowywanie i przetwarzanie danych biometrycznych (skany linii papilarnych, twarzy czy tęczówki). SPU ma działać całkowicie niezależnie od systemu operacyjnego urządzenia.

BUDOWA JEDNOSTKI DYNAMIQ SHARED UNIT (DSU)



Oznacza to dużą elastyczność w projektowaniu nowych procesorów. Należy jednak pamiętać, że każda domena wymaga osobnego regulatora napięcia, co ma wpływ na złożoność układu i podraża jego koszty.

Podstawowym modułem odpowiedzialnym za działanie omawianej technologii jest DynamIQ Shared Unit (DSU) – przypisana do każdego klastra jednostka operacyjna odpowiedzialna za komunikację poszczególnych rdzeni w klastrze pomiędzy sobą i całego klastra z resztą systemu. Każda domena w klastrze może komunikować się z DSU w trybie synchronicznym lub asynchronicznym. Działanie w trybie asynchronicznym umożliwia pracę rdzeni z różnymi częstotliwościami, podczas gdy komunikacja w trybie synchronicznym wymusza pracę wszystkich rdzeni domeny z jedną częstotliwością.

Poszczególne rdzenie p**osiadają teraz własną pamięć cache drugiego poziomu (L2), DSU obsługuje natomiast pamięć cache trzeciego poziomu (L3) wspólną dla wszystkich rdzeni**. Samo przesunięcie pamięci cache L2 „bliżej" rdzeni powinno zwiększyć jej wydajność o 50%. L3 cache ma współpracować z pamięcią L2 w trybie pseudo-exclusive, co oznacza, że (prawie zawsze) będą w niej przechowywane tylko te dane, które nie będą znajdować się w pamięci L2.

Pamięć L3 może być podzielona maksymalnie na cztery grupy, przy czym grupy te mogą mieć różne rozmiary i być przypisane do jednego lub wielu rdzeni albo zewnętrznych układów podłączonych do DSU. Ponadto L3 cache może być zarządzana i partycjonowana z poziomu systemu operacyjnego lub hypervisora.

DSU minimalizuje opóźnienia i optymalizuje przepływ danych, a także zarządza energią klastra. Z dodatkowych cech należy wymienić sprzętowe raportowanie błędów, obsługę ECC/parzystości przez pamięć L3, specjalny tryb schowka w pamięci cache L3 (cache stashing) pozwalający na bezpośredni dostęp do niej z poziomu GPU i innych układów wejścia/wyjścia oraz ulepszone zarządzanie energią.

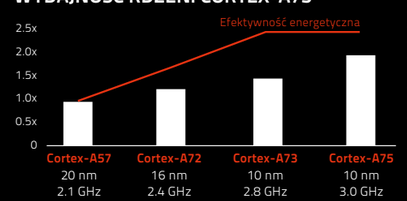
Do pracy w nowej organizacji SoC przewidziano nowe rodzaje rdzeni – odpowiednio A75 przeznaczony do zadań wymagających wysokiej wydajności oraz A55 do pracy w trybie oszczędzania energii.

Lista urządzeń, które zostaną wyposażone w procesor Qualcomm Snapdragon 845: Samsung Galaxy S9/S9+, LG G7/G7+, Xiaomi Mi 7, HTC U12, OnePlus 6, Nubia Z18, Sony Xperia XZ Pro, Samsung Galaxy Note 9, Xiaomi Mi Mix 3, LG V40, Google Pixel 3, Google Pixel 3 XL, Nubia Z18S, Sony Xperia XZ2, HTC U12+, Motorola Moto Z 2019, OnePlus 6T i Samsung W2019.

PODSUMOWANIE

Nowy Snapdragon 845 to jedna z największych zmian w architekturze systemów ARM SoC na przestrzeni ostatnich lat, w ramach której po raz pierwszy zastosowano nową technologię klastrowania rdzeni DynamIQ. Snapdragon 845 „na papierze" spełnia większość pokładanych w nim nadziei. Ponieważ jego poprzednik – Snapdragon 835 był już bardzo dobrym układem, w którym projektantom udało się idealnie zrównoważyć wydajność i pobór energii, sukces Snapdragona 845 wydaje się przesądzony. Jeśli wszystko pójdzie zgodnie z planem, prawdopodobnie w tym roku zobaczymy kolejną generację bardzo dobrych urządzeń mobilnych, na które wszyscy niecierpliwie czekamy.

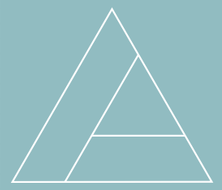
WYDAJNOŚĆ RDZENI CORTEX-A75



KRAJOBRAZ ZAGROŻEŃ **DLA APLIKACJI**

Aplikacje są podstawą niemal każdego biznesu. Instalowane na urządzeniach lub dostępne z chmury pozwalają m.in. organizować i rozwijać firmę, zachować konkurencyjność, analizować dane, komunikować się pracownikom, budować relacje z klientami. Aplikacje zwiększają produktywność i szybkość wdrażania innowacji, ale są też celem przestępców i furtką, przez którą mogą wyciec dane, narażając bezpieczeństwo użytkowników i reputację organizacji.

Sebastian Kuniszewski



W zmieniającym się krajobrazie cyfrowych zagrożeń i możliwości równoważenie korzyści wynikających z wdrażania nowych rozwiązań, z utrzymaniem odpowiedniego poziomu bezpieczeństwa, może przypominać planowanie i prowadzenie działań wojennych. Może, ale wcale nie musi.

DOBRY PUNKT WYJŚCIA

Zrozumienie kontekstu działania aplikacji i miejsc, w których mogą być one szczególnie narażone na ataki, to decydujący punkt wyjściowy. Analizując stan firmowego ekosystemu IT, należy przyjrzeć się: sieci, w której udostępniana jest/działa aplikacja;

22%

– o tyle procent wzrosła liczba ataków na aplikacje internetowe w 2017 r. w porównaniu z 2016 r.

(źródło: Verizon Insights Lab)

danym, które użytkownik przesyła do aplikacji; serwerowi DNS, który przetwarza adresy IP potrzebne do uzyskania dostępu do aplikacji; serwerom internetowym w przypadku, gdy są używane przez aplikacje oraz powiązanym interfejsom API wykorzystywanym przez inne aplikacje i systemy. Konieczne jest wykorzystanie dostępnych informacji o zagrożeniach do rozpoznawania najbardziej krytycznych luk danej aplikacji. Taka kontrola infrastruktury będzie pomocna niezależnie od sytuacji, gdy to aplikacja będzie głównym celem ataku, czy też będzie ona elementem użytym do przeprowadzania ataków na większą skalę (przykładem są botnety IoT). Konieczne jest też nieustanne zdobywanie wiedzy, dzięki któremu możliwe jest wdrażanie rozwiązań, które najlepiej ochronią organizację przed zagrożeniami we wszystkich punktach, w których aplikacja jest narażona na atak. Wymienione działania pozwalają zadbać o poufność, integralność, a także dostępność używanych aplikacji i danych.

PROFIL RYZYKA DLA BRANŻY

Różnorodne złośliwe oprogramowanie zawsze ma na celu ułatwienie przestępcom osiągnięcia ostatecznego celu, którym jest zysk finansowy, rejestracja urządzenia w botnecie, rozprowadzenie spamu lub przejęcie konta. Trojany, wirusy, darmowe oprogramowanie z reklamami i rootkity są wszechobecne. Wykorzystuje się je wszędzie i do wszystkiego, łącznie z oszustwami internetowymi, kradzieżą danych uwierzytelniających i budową botnetów, używanych do przeprowadzania ataków DDoS. Kluczem do zarządzania ryzykiem pod kątem złośliwego oprogramowania jest zrozumienie profilu ryzyka dla branży, a także poznanie rodzajów złośliwego oprogramowania wykorzystywanego przez potencjalnie zagrażające firmie jednostki. Jak podano w raporcie firmy F5 pt. „The-Evolving-Risk-Landscape" w pierwszym kwartale 2017 r. nowy rodzaj złośliwego oprogramowania pojawiał się co 4,2 sekundy, a ponad połowa (51%) wszystkich naruszeń w 2016 r. była związana z jakąś formą złośliwego oprogramowania.

66%

złośliwego oprogramowania zostało zainstalowane za pośrednictwem złośliwych załączników do wiadomości e-mail. (źródło: F5)

Tradycyjne rozwiązania wykrywające złośliwe oprogramowanie, takie jak programy antywirusowe i czarne listy, nie są wystarczająco skuteczne wobec rozprzestrzenianych obecnie zagrożeń – konieczne jest stosowanie kombinacji rozwiązań udostępniających mechanizmy analizy behawioralnej i analizy zagrożeń. Pomocne są również takie mechanizmy i działania jak:

- ochrona systemu i użytkownika za pomocą piaskownicy (wymuszanie otwarcia załączników lub łączy w izolowanym środowisku);
- ocena oprogramowania za pomocą wspomnianej analizy behawioralnej, badającej sposób działania oprogramowania, a nie tylko sygnatury plików;
- ograniczanie uprawnień (np. blokada możliwości instalowania oprogramowania przez większość użytkowników);
- białe listy aplikacji.

Rozprzestrzenianie się złośliwego oprogramowania ogranicza też (bez jednoczesnego zwiększania obciążenia działu IT) umiejętność rozpoznawania przez użytkowników oszustw oraz witryn i usług dystrybuujących złośliwe oprogramowanie, a także łatwo dostępne firmowe repozytoria zawierające bezpieczne i zatwierdzone do użycia oprogramowanie.

BANALNY I NIEBEZPIECZNY

Według statystyk głównym sposobem dostarczania oprogramowania ransomware i innych rodzajów złośliwego oprogramowania jest phishing, który nie jest łatwo jednoznacznie zdefiniować. Oszustwa phishingowe mają nakłonić użytkowników do kliknięcia łącza, które może zainfekować ich system złośliwym oprogramowaniem lub przenieść na fałszywą stronę internetową, przeznaczoną do kradzieży danych osobowych. Phishing może

też pomóc cyberprzestępcom przejąć konta użytkowników, uzyskać dostęp do poufnych danych i ukraść pieniądze lub inne środki (punkty z kart lojalnościowych, mile lotnicze itp.). Ponadto w atakach phishingowych podstępem skłania się użytkownika do zainstalowania złośliwego oprogramowania sterującego i kontrolującego, które może otworzyć hakerom drzwi do sieci korporacyjnych.

Niestety, nie ma jednego skutecznego rozwiązania, które powstrzymałoby ataki phishingowe. Jedynym wyjściem jest szkolenie użytkowników, jak rozpoznawać tego typu e-maile i co zrobić, jeśli przez pomyłkę dadzą się oszukać. Pomocne jest też informowanie o pojawiających się atakach phishingowych oraz wdrożenie narzędzi ułatwiających użytkownikom natychmiastowe zgłaszanie incydentu do działu IT, jeśli podejrzewają, że kliknęli link ze złośliwym oprogramowaniem lub omyłkowo ujawnili swoje dane uwierzytelniające.

KOMPLETNA OCHRONA

Czasy, w których jednopunktowe rozwiązania wystarczały do ochrony przed zagrożeniami, dawno minęły. Aplikacje dostarczane są z i do różnych miejsc, takich jak centra danych, prywatne chmury, chmury publiczne, kontenery, platformy SaaS – niezbędne jest więc zintegrowane podejścia do ochrony infrastruktury, oprogramowania i danych. Dzięki analizie pojawiających się zagrożeń, wykorzystywaniu i udostępnianiu informacji o zagrożeniach oraz dostosowaniu rozwiązań zabezpieczających do rzeczywistych potrzeb można stworzyć kompleksowy program bezpieczeństwa.

Tylko w ciągu pierwszych sześciu miesięcy 2017 r. zgłoszono 2227 naruszeń, które naraziły na niebezpieczeństwo ponad 6 miliardów danych

(źródło: darkreading.com)

ATAKI CREDENTIAL STUFFING – DANE UŻYTKOWNIKÓW DROŻSZE NIŻ NUMERY KART KREDYTOWYCH

Wraz z rosnącą liczbą incydentów związanych z bezpieczeństwem każdego roku kradzionych jest coraz więcej danych uwierzytelniających. Jak podsumowuje firma F5 w raporcie pt. „The-Evolving-Risk-Landscape", zestawy nazw użytkowników i haseł sprzedawane są ponad 17 razy drożej niż skradzione numery kart kredytowych! Oznacza to, że kradzież danych uwierzytelniających to lukratywny interes. Podczas ataku typu **credential stuffing** przestępcy wykorzystują skradzione dane użytkowników i hasła oraz podejmują wielokrotne próby uzyskania dostępu do kont użytkowników korporacyjnych lub klientów. Według danych darkreading.com tylko w ciągu pierwszych sześciu miesięcy 2017 r. zgłoszono 2227 naruszeń, które naraziły na niebezpieczeństwo ponad 6 miliardów danych.

Przed atakami typu credential stuffing można chronić swoją firmę, szkoląc pracowników i wzmacniając mechanizmy obronne. Z uwagi na to, że większość tego typu ataków jest realizowana przy użyciu zautomatyzowanych programów, warto wdrożyć w firmie zaawansowane mechanizmy wykrywania botów i zapobiegania ich działaniu m.in. w taki sposób jak:

- zaprojektowanie formularza logowania do swojej witryny z zastosowaniem dynamicznej obfuskacji (boty nie będą w stanie rozpoznać właściwych pól i automatycznie wstawiać skradzionych danych uwierzytelniających);
- włączenie szyfrowania danych przesyłanych do i z przeglądarki WWW oraz stosowanych w firmie aplikacji mobilnych (w przypadku przechwycenia dane będą bezwartościowe);
- wykorzystywanie mechanizmów pojedynczego logowania (single sign-on, SSO) oraz uwierzytelniania wielopoziomowego za pośrednictwem scentralizowanej bramy dostępu;
- monitorowanie nieudanych prób uwierzytelnienia i klasyfikowanie ich źródeł w celu ułatwienia identyfikacji i blokowania zainfekowanych punktów końcowych.

51%

wszystkich naruszeń w 2016 r. było związanych z jakąś formą złośliwego oprogramowania.

(źródło: F5)

APLIKACJE – RODZAJE ZAGROŻEŃ

USŁUGI ZWIĄZANE Z APLIKACJĄ

- Ataki XSS (cross-site scripting)
- Ataki CSRF (cross-site request forgery)
- Ataki SQL Injection
- Złośliwe oprogramowanie
- Ataki DoS (blokada usług)
- Ataki interfejsów API
- Ataki MITM (man in the middle)
- Wykorzystanie funkcjonalności

PROTOKÓŁ TLS/SSL

- Ataki związane z ujawnianiem pamięci
- Spoofing certyfikatu
- Przechwytywanie sesji
- Wykorzystywanie protokołów

SIEĆ

- Ataki DDoS
- Podsłuch
- Wykorzystywanie protokołów

KLIENT

- Ataki CSRF (cross-site request forgery)
- Ataki MITB (man in the browser)
- Ataki XSS (cross-site scripting)
- Złośliwe oprogramowanie
- Ataki SQL Injection

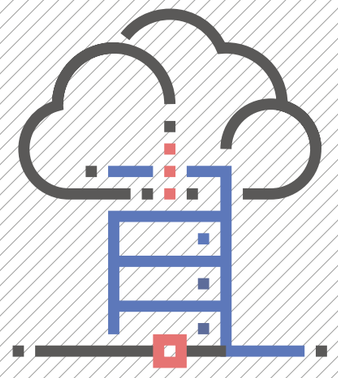
DOSTĘP

- Kradzież danych uwierzytelniających
- Ataki typu credential stuffing
- Przechwytywanie sesji
- Ataki brute force
- Phishing

SERWER DNS

- Zatruwanie serwera dns
- Spoofing serwera dns
- Przechwytywanie serwera dns
- Ataki słownikowe
- Ataki DDoS

USŁUGI CHMURY PUBLICZNEJ – NOWE INWESTYCJE, WYZWANIA, OBAWY



Dynamika sprzedaży rozwiązań w chmurze rośnie od czterech lat. Coraz większy wpływ na te wyniki ma szybsza adaptacja cloud computingu w Europie Środkowo-Wschodniej, w tym także w Polsce. Równocześnie niejasną kwestią dla wielu firm pozostaje odpowiedzialność za bezpieczeństwo zasobów, a niepokój podkreślają inwestycje w dodatkowe zabezpieczenia.

Sebastian Kuniszewski

Coraz większy udział w przychodach dostawców usług chmurowych mają kraje Europy Środkowo-Wschodniej, w tym również Polska. W ubiegłym roku tylko w naszym kraju podpisano dziesiątki dużych umów na wdrożenie usług chmurowych – przede wszystkim w zatrudniających powyżej 250 pracowników przedsiębiorstwach. Co ciekawe, na zbliżonym poziomie kształtowało się zainteresowanie rozwiązaniami PaaS, IaaS oraz SaaS.

WZROSTY I SPADKI – ZMIANA PUNKTU WIDZENIA

Rosnącą popularność chmury obliczeniowej w regionie potwierdzają dane firmy analitycznej IDC, która zwraca uwagę na dwa ważne wnioski: po pierwsze, wartość rynku IT w ciągu najbliższych 4 lat będzie systematycznie rosła, choć nie wszędzie w takim samym tempie. IDC prognozuje, że wzrost wydatków na IT w latach 2016-17 w największym stopniu odczuwalny będzie w Polsce i wyniesie 3,7%. Dla porównania, w Czechach nie przekroczy on 1,9%, w Rosji odczuwalny będzie spadek o ponad 2%.

W 2016 r. wartość rynku IT w Europie Środkowo-Wschodniej wyniosła 38 miliardów dolarów i w 2020 r. wg szacunków ma osiągnąć już 44 mld dolarów. Ale nie wzrost nakładów jest najistotniejszy. Ciekawszy jest drugi wniosek – o ile udział outsourcingu IT w 2016 r. wynosił 38%, o tyle w 2020 r. wzrośnie on do 44%. W tym samym czasie udział tradycyjnych usług IT spadnie z 63% do 57%. Największy wzrost będzie dotyczył outsourcingu infrastruktury z 10 do 14%, w tym niemal dwukrotny wzrost wartości usług w chmurze – z 2,6% do 4,6%. W największym stopniu spadną natomiast nakłady na infrastrukturę klienta – z 23% do 20% w ciągu 4 najbliższych lat.

Z badania przeprowadzonego na zlecenie Oracle wynika, że z chmury korzysta obecnie już 40% firm z regionu, zatrudniających od 250 do 1000 pracowników. Natomiast niemal połowa firm zatrudniających ponad 2500 osób i 41% przedsiębiorstw zatrudniających od 1000 do 2500 pracowników planuje wdrożenie usług w chmurze lub ocenia możliwość ich zastosowania.

– Oceniamy, że za kilka lat usługi chmury publicznej staną się tak powszechne jak obecnie internet. Doświadczenia pokazują bowiem, że chmura daje ogromne korzyści w postaci nie tylko mniejszych kosztów, ale też szybkości wdrożenia czy większego bezpieczeństwa danych. I co najważniejsze – przedsiębiorcy to dostrzegają i tematu chmury już nie bagatelizują – mówi Janusz Naklicki, szef regionu Oracle CEE & CIS.

JANUSZ NAKLICKI,
szef regionu Oracle CEE & CIS

Cyfrowa transformacja firm przestaje być marketingowym sloganem, staje się faktem. Także w Polsce, gdzie firmy coraz częściej rezygnują z tradycyjnych wdrożeń na rzecz usług chmurowych. Z analiz Oracle wynika, że rynek usług chmurowych rośnie obecnie około pięć razy szybciej niż inwestycje w systemy tradycyjne. Największy potencjał widzimy na rynku użyteczności publicznej, finansowym oraz telekomunikacyjnym.

WSCHÓD I ZACHÓD – INNA SKALA, TE SAME OBAWY

Dane pokazują, że mimo optymistycznych prognoz i odczuwalnego wzrostu inwestycji w chmurę dystans pomiędzy Europą Środkowo-Wschodnią a Zachodnią pod względem adaptacji chmury jest znaczny i będzie się zwiększał. Jak prognozuje IDC, w 2017 r. wydatki na chmurę prywatną i publiczną w regionie wyniosą 594 mln dolarów, a w 2020 r. wzrosną do 876 mln dolarów. Dla porównania wydatki na chmurę w Europie Zachodniej wzrosną w tym czasie z 6,19 mld dolarów do 9,11 mld dolarów, a do końca 2017 r. aż 80% globalnych firm zainicjuje projekty w zakresie cyfrowej transformacji. To poważne wyzwanie i sygnał dla polskich przedsiębiorstw. – Brak przemyślanych inwestycji w chmurę grozi tym, że polskie firmy, a co za tym idzie, gospodarka, będą mniej innowacyjne. Przedsiębiorstwa, które to rozumieją, w krótkim czasie zdeklasują konkurencję – podkreśla Naklicki.

Coraz większym inwestycjom w usługi cloudowe towarzyszą obawy związane z bezpieczeństwem zasobów oraz odpowiedzialnością dostawców usług za ochronę danych organizacji. Te przeciwstawne odczucia wyraźnie wybijały się z badania pt. „Steps to Secure Your Journey to the Public Cloud", przeprowadzonego na zlecenie Barracuda Networks wśród menedżerów IT. O opinie poproszono 550 osób decyzyjnych z działów IT w organizacjach z regionu EMEA, wykorzystujących chmurę publiczną w modelu IaaS. Badanie, które sprawdzało adaptację chmury publicznej na o wiele większym obszarze niż tylko Europa Środkowo-Wschodnia, przeprowadzono w kwietniu i maju 2017 r.

Odpowiedzialność za bezpieczeństwo pozostaje często niejasną kwestią, a inwestycje w dodatkowe zabezpieczenia podkreślają ciągły niepokój klientów.

ADAPTACJA CHMURY W EMEA – KLUCZOWE TRENDY

- 20% budżetów IT przeznaczanych jest obecnie na wdrożenia w chmurze publicznej. Organizacje oczekują, że w ciągu dwóch lat połowa ich infrastruktury znajdzie się w chmurze publicznej;
- 45% respondentów uważa, że ich dostawca usług IaaS w chmurze publicznej jest w pełni zdolny do zapewnienia skutecznej ochrony, jeśli chodzi o dostęp do aplikacji chmurowych;
- 57% respondentów twierdzi, że zainwestowało w dodatkowe produkty zabezpieczające, żeby chronić dostęp do chmury publicznej, a kolejne 37% badanych planuje takie działania zrealizować w przyszłości;
- Wśród firm z regionu EMEA najpopularniejsze jest wykorzystanie chmury publicznej do przechowywania (77%) i przywracania danych (56%). Na kolejnych pozycjach wymieniano hosting stron internetowych i aplikacji (54%), analitykę danych (51%) i systemy CRM (46%);
- Wbrew założeniom modelu współdzielonej odpowiedzialności ponad 60% respondentów uważa, że za zabezpieczenie danych w chmurze, aplikacji i systemów operacyjnych odpowiada dostawca usług.

Źródło: „Steps to Secure Your Journey to the Public Cloud", Barracuda Networks

IMPLEMENTACJA USŁUG CHMUROWYCH W EMEA – GŁÓWNE OBSZARY

77% – pamięci masowe
56% – odzyskiwanie danych
54% – hosting stron i aplikacji
48% – poprawa skalowalności usług chmury publicznej
38% – wykorzystanie chmury publicznej do testowania i rozwijania aplikacji
33% – użycie chmury publicznej do wirtualizacji desktopów
27% – użycie chmury publicznej do rozwoju usług/produktów i ich testowania

POPULARNOŚĆ CHMURY I OBAWY O BEZPIECZEŃSTWO

Przedstawiciele badanych firm z regionu EMEA, które używają usług w modelu IaaS, twierdzą, że niemal 35% ich infrastruktury obecnie znajduje się w chmurze, a udział ten ma wzrosnąć do 50% w ciągu najbliższych dwóch lat. Najniższy udział chmury publicznej w infrastrukturze występuje w Wielkiej Brytanii (29%), która pozostaje w tyle za Austrią (35%), Niemcami (35%), Francją (38%) oraz Belgią i Holandią (41%).

Spośród firm, które zdecydowały się korzystać z chmury publicznej, niespełna połowa (45%) ma pewność, że ich dostawca jest w pełni zdolny do zapewnienia skutecznej ochrony dostępu do aplikacji chmurowych, a podobny odsetek twierdzi to samo o skutecznej ochronie samych aplikacji działających w chmurze (43%) oraz przetwarzanych w niej danych (41%). Wyraźnie widać więc, że duży odsetek użytkowników nie jest pewien poziomu bezpieczeństwa, jaki oferuje ich dostawca usług. Tylko rozwiązanie tego problemu – zarówno w kwestii uświadamiania klientów, sposobu konstruowania umów, jak i stosowania odpowiednich zabezpieczeń – pozwoli utrzymać dynamikę wzrostu. – Pomimo rosnącej popularności chmury publicznej w całym regionie EMEA obawy o bezpieczeństwo pozostają poważne. 77% respondentów twierdzi, że używa chmury publicznej do przechowywania takich danych, jak informacje o pracownikach, własność intelektualna firmy oraz informacje bankowe o klientach, a unijne ogólne rozporządzenie o ochronie danych osobowych (rodo), które wejdzie w życie w maju 2018 r., jeszcze dobitniej zwraca uwagę na konieczność odpowiedniej ochrony informacji przetwarzanych w chmurze – podkreśla Kristof Vanderstraeten, dyrektor ds. rozwoju działalności związanej z chmurą publiczną na region EMEA w Barracuda Networks.

BRAK ZROZUMIENIA A ZWIĘKSZONE RYZYKO

Z badania wynika też, że wielu decydentów IT nie zna dokładnie swoich obowiązków w zakresie zapewnienia bezpieczeństwa zasobów przetwarzanych w chmurze. Tylko 61% respondentów stwierdziło, że w pełni rozumie swoje obowiązki w tym obszarze – przy podziale na konkretne kraje liczba ta wzrasta do 69% w Niemczech i spada do 51% w Belgii i Holandii.

Bardziej niepokojące jest to, że niemal dwie trzecie respondentów z regionu EMEA uważa, że za zabezpieczenie danych w chmurze wyłącznie odpowiada dostawca usług. 61% mówi to samo o aplikacjach i 60% o systemach operacyjnych. Podkreśla to nieznajomość modelu współdzielonej odpowiedzialności – Shared Responsibility Model – kluczowego postanowienia większości umów z dostawcami usług chmurowych. Zgodnie z nim dostawca zabezpiecza podstawowe komponenty infrastruktury, takie jak: zasoby obliczeniowe, pamięć masowa, bazy danych, łączność sieciowa oraz fizyczne obiekty, podczas gdy obowiązkiem klienta jest zabezpieczenie danych, aplikacji, systemów operacyjnych oraz innego oprogramowania działającego w chmurze.

Pomimo tej nieświadomości ryzyka pocieszające jest to, że firmy inwestują w dodatkowe zabezpieczenia. 57% respondentów twierdzi, że wdrożyło dodatkowe produkty zabezpieczające dostęp do chmury publicznej, a kolejne 37% badanych planuje to zrobić w niedalekiej przyszłości. Najczęściej dodatkowe zabezpieczenia stosowane są w Belgii i Holandii (70% badanych), a najrzadziej w Wielkiej Brytanii (43%).

KRISTOF VANDERSTRAETEN
dyrektor na region EMEA w Barracuda Networks

Z naszego badania jasno wynika, że chmura publiczna jest atrakcyjną propozycją, ale migracja wrażliwych aplikacji biznesowych bywa skomplikowanym procesem, który generuje nowe wymagania i wyzwania w zakresie bezpieczeństwa. Wsłuchaliśmy się w te obawy i wprowadzamy nowości w programie Barracuda Cloud Ready, z którego organizacje mogą korzystać bezpłatnie w ramach 90-dniowej licencji chmurowej na Barracuda Web Application Firewall oraz Barracuda NextGen Firewall w chmurach AWS i Microsoft Azure.

35%

organizacji z regionu EMEA zaczęło już migrację zasobów do chmury. 26% z nich osiąga zwrot z inwestycji już w pierwszym roku korzystania z usług chmurowych.

NOWE TRENDY W DRUKOWANIU

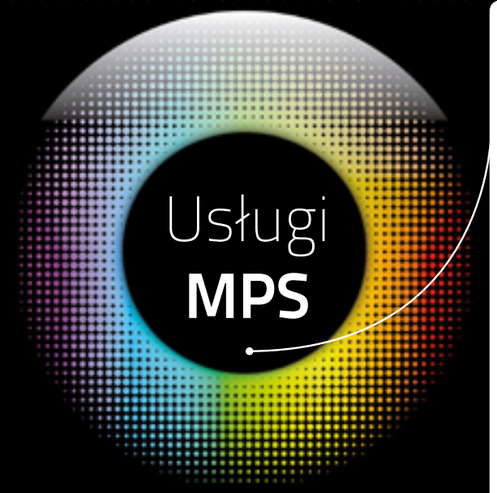
Chociaż postęp w branży poligraficznej i technologii związanych z drukiem nie jest spektakularny, to jednak rynek ten dynamicznie się rozwija – zarówno w sferze technologii, jak i zarządzania czy organizacji druku, co wpływa na wzrost jakości usług przy jednoczesnym obniżeniu kosztu i czasu ich realizacji. Wśród najważniejszych trendów można wymienić zjawiska BYOD i druk mobilny, rosnącą popularność usług z zakresu zarządzania drukiem (MPS), czy rozwój technologii nanograficznej.

Jerzy Michalczyk

Cyfryzacja i rozwój nowych technologii nie omijają rynku druku. Dzięki temu drukowanie jest dziś coraz bardziej efektywne – zarówno pod kątem jakości, bezpieczeństwa, czasu, jak i związanych z nim kosztów.

Bring Your Own Device to trend będący wynikiem przenikania się życia zawodowego z prywatnym. Polega on na korzystaniu z prywatnych urządzeń czy serwisów w celach biznesowych. Pracownik może dziś za pomocą telefonu czy tabletu zdalnie zlecać i kontrolować druk – nawet będąc kilkaset kilometrów od urządzenia drukującego. Co się z tym wiąże, urządzenia drukujące są dziś nie tylko wielofunkcyjne, ale i kompatybilne z większą liczbą sprzętu niż dotychczas.

Kwestia mobilnego drukowania wiąże się z innym rozwiązaniem w sferze druku – możliwością drukowania bezpośrednio z wirtualnej chmury. Choć usługa ta nie jest nowością na rynku, to z racji dynamicznego rozwoju wciąż zaliczana jest do panujących na nim trendów. Liczba potencjalnych zastosowań oraz zalet druku z wirtualnej chmury jest bardzo duża – od optymalizacji procesów drukowania, przez intuicyjność i łatwość obsługi, aż po oszczędność czasu oraz kosztów. Z wirtualną chmurą wiążą się z kolei usługi zarządzania drukiem, czyli MPS, które wkraczają do coraz większej liczby firm, niezależnie od ich wielkości. Oprogramowania do zarządzania drukiem działają zwykle właśnie w oparciu o wirtualną chmurę.



Usługi zarządzania drukiem (Managed Print Services, MPS) to korzystanie z zewnętrznego dostawcy do oceny, optymalizacji i ciągłego zarządzania środowiskiem druku w organizacji. Dzięki takim rozwiązaniom przedsiębiorstwa mogą obniżyć koszty i zwiększyć wydajność pracy. Całkowite koszty drukowania w biurze są zazwyczaj głównym, niekontrolowanym wydatkiem firmy, rozkładającym się na wiele działów. Szacuje się, że średniej wielkości przedsiębiorstwa dzięki wykorzystaniu programów do zarządzania dokumentami będą w stanie zaoszczędzić ponad 100 000 dolarów w okresie pięciu lat. Nic więc dziwnego, że rozwiązania MPS cieszą się coraz większym zainteresowaniem firm. Efektywne zarządzanie dokumentami może mieć znaczący wpływ na optymalizację kosztów operacyjnych w firmie oraz maksymalizację wydajności pracy. Agencja badawcza Gartner przewiduje, że do 2020 roku ponad 70% przedsiębiorstw zatrudniających 250 i więcej pracowników zacznie korzystać z usług zarządzania drukiem.

Zaawansowane rozwiązania z zakresu MPS pozwalają obecnie na dokładne rozpoznanie aktualnych kosztów drukowania, umożliwiają kontrolę urządzeń, także pod kątem eksploatacji, zdalne administrowanie drukiem, dokładne rozliczanie kosztów oraz dbanie o bezpieczeństwo wydruku. Jednocześnie rozwiązania te są coraz bardziej intuicyjne i nie wymagają dodatkowego zaangażowania pracowników z działu IT.

– Łukasz Laskowski, prezes zarządu firmy Ediko

przedsiębiorstw zatrudniających 250 i więcej pracowników według agencji Gartner zacznie korzystać z usług zarządzania drukiem.

Zarządzanie drukiem w przedsiębiorstwie

Początkowo usługi MPS koncentrowały się na sprzęcie do drukowania, dostawach, wielkości wydruku i kosztach drukowania. Obecnie celem jest dostarczenie firmom pełnego obrazu środowiska druku, dostarczającego nie tylko wiedzy o tym, jak drukowane zasoby są przydzielane, ale również w jaki sposób dokumenty są używane, kiedy i gdzie są drukowane, dzięki jakim aplikacjom i jakie jest ich przeznaczenie.

Według badań instytutu badawczego Gartner koszty druku odpowiadają za 3 do 5 proc. obrotów firmy w skali roku. W biurach polskich firm marnotrawionych jest około 8 proc. wszystkich drukówm, co oznacza, że jeden pracownik miesięcznie generuje stratę na poziomie 50 kartek papieru. Dzięki zastosowaniu nowoczesnych rozwiązań MPS można zaoszczędzić nawet do 40 proc. kosztów, uzyskując tym samym kontrolę nad drukowaniem oraz zwiększając produktywność i ochronę informacji poufnych.

Zatem firmy ściśle współpracujące z dostawcami rozwiązań MPS uzyskają gwarancję, że zmiany wprowadzane w infrastrukturze środowiska druku dostosowane są do strategicznych celów i zadań w zakresie oszczędności, wydajności, efektywności procesów biznesowych, a także bezpieczeństwa.

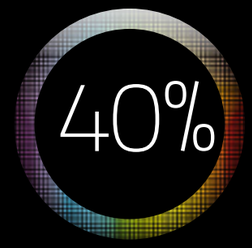
Korzyści wynikające ze stosowania rozwiązań z obszaru MPS

- Zwiększona kontrola nad całkowitymi kosztami drukowania, obniżenie kosztów druku;
- Automatyzacja i usprawnienie procesów biznesowych;
- Maksymalizacja żywotności urządzeń drukujących;
- Proaktywne monitorowanie urządzeń i wydatków w czasie rzeczywistym;
- Zwiększenie produktywności użytkowników urządzeń;
- Minimalizacja zaangażowania pracowników IT w obsługę urządzeń drukujących;
- Optymalizacja kosztów administracyjnych;
- Wzrost świadomości użytkowników na temat kosztów druku.

Druk nanograficzny

Rozwój technologii poligraficznych dotyczy nie tylko usprawnienia procesu drukowania oraz optymalizacji jego zabezpieczeń, ale w dużej mierze wiąże się również z poprawą jakości samego druku. Jedną z nowinek na rynku jest druk nanograficzny. W procesie druku nanograficznego zasadniczą rolę odgrywa tusz. Dzięki zastosowaniu nanopigmentów składających się z cząstek, których wielkość mierzy się w dziesiątych częściach nanometra (ludzki włos jest grubości ok. 100 tys. nanometrów), uzyskuje się wyższą, szerszą przestrzeń barw, a dzięki niej – lepsze odwzorowanie kolorów oraz wyższą ostrość obrazu niż w innych typach druku. Wydruki nanograficzne odznaczają się dużą odpornością na ścieranie i na zadrapania. Drukować można na wszystkich rodzajach podłoży, papierach powlekanych i niepowlekanych, tekturze makulaturowej, papierze gazetowym, foliach z tworzyw sztucznych bez obróbki wstępnej czy specjalnej warstwy podłożowej i utrwalania. Technologia nanograficzna znajduje już zastosowanie w produkcji książek, czasopism, etykiet, opakowań spożywczych czy produktów farmaceutycznych i kosmetyków.

Szczególną zaletą tego typu druku jest jego opłacalność. Koszt wydrukowania jednej strony jest niższy niż przy użyciu jakiejkolwiek innej technologii. Co ciekawe, proces druku nanograficznego wykorzystuje tusze wodorozcieńczalne, nie tylko efektywne energetycznie, ale również przyjazne dla środowiska.



o tyle można zmniejszyć koszty druku dzięki zastosowaniu nowoczesnych rozwiązań **MPS**.

Bezpieczeństwo druku

Efektywna administracja środowiskiem druku zajmuje coraz ważniejszą pozycję w procesie zarządzania przedsiębiorstwem. Nowoczesne systemy bezpieczeństwa muszą tym samym uwzględniać różne aspekty działalności firm i funkcjonować na wielu płaszczyznach. Jednak duża część zagrożeń, które są związane z technologią informacyjną, wynikają nie z ograniczeń technologicznych, ale z czynnika ludzkiego. W związku z tym działania mające na celu zabezpieczenie poufności dokumentów, zwłaszcza drukowanych, należy skoncentrować na zdefiniowaniu procedur bezpieczeństwa, ich przestrzeganiu i edukacji pracowników.

– Maciej Nuckowski, dyrektor Działu Usług w Xerox Polska

MAKE INTERNET FASTER

300 milionów dolarów kosztowała konsorcjum złożone z koncernów: Google, China Mobile International, China Telecom Global, Global Transit, KDDI i Singtel inwestycja, której celem było połączenie USA i Japonii transoceanicznym kablem światłowodowym. Dzięki temu świat zyskał w czerwcu br. najszybszą „rurę" do przesyłania danych o przepustowości 60 Tbps. Nowy kabel nazwano Faster.

Jerzy Michalczyk

W czerwcu Microsoft i Facebook rozpoczęły także budowę przewodu Marea, który połączy USA i Europę. Inwestycja ma zostać zakończona już w 2017 roku, a planowana prędkość transmisji ma wynieść aż 160 Tbps. Ogólna szybkość łączy podmorskich sięga obecnie 300 Tbps, ale i tak stanowić to będzie ułamek wydajności połączeń śródlądowych. Po co nam takie szybkie łącza? Aby sprostać popytowi na przepustowość, jaki pojawi się w najbliższych latach.

Zgodnie z danymi prezentowanymi przez firmę Cisco w raporcie **Visual Networking Index** całkowite zapotrzebowanie na transfer w roku 2020 ma sięgnąć niemal 200 eksabajtów na sekundę, a ruch IP w stosunku do stanu z początku tego roku ma wzrosnąć trzykrotnie! Jeszcze większy wpływ na wzrost ruchu IP będzie miała globalna transformacja cyfrowa, w wyniku której w roku 2020 światowe sieci IP będą obsługiwać o 10 miliardów urządzeń i połączeń M2M (machine-to-machine) więcej niż w roku 2015 (wzrost z 16,3 mld do 26,3 mld). Na jednego mieszkańca globu w roku 2020 przypadać będzie 3,4 urządzenia (w roku 2015 było to 2,2). Światowa społeczność użytkowników internetu wzrośnie w tym okresie o ponad miliard osób – z 3 miliardów w roku 2015 do 4,1 mld w roku 2020. Oto więcej szczegółów tego raportu:

- stabilny wzrost ruchu IP – ruch IP wzrośnie trzykrotnie w ciągu najbliższych 5 lat, ruch w internecie w godzinach szczytu rośnie szybciej niż średnia ruchu w internecie. Ruch w godzinach szczytu wzrośnie w latach 2015 niemal pięciokrotnie;
- łącza szerokopasmowe – szybkość stałych łączy szerokopasmowych wzrośnie dwukrotnie – z 24,7 Mb/s do 47,7 Mb/s;
- ruch generowany przez smartfony wyprzedzi ruch generowany przez komputery – zmienia się sposób, w jaki użytkownicy indywidualni i biznesowi łączą się z internetem. Do 2020 roku 71% całego ruchu IP pochodzić będzie z urządzeń innych niż komputery: smartfonów, tabletów czy telewizorów (w porównaniu z 47% w roku 2015). Do roku 2020 smartfony będą generować 30% całkowitego ruchu w sieciach IP, podczas gdy udział ruchu z komputerów w całkowitym ruchu IP spadnie do 29%;
- korzystanie z usług interneto-wych – ruch związany z grami w internecie będzie najszybciej rozwijającą się usługą w domowym internecie konsumenckim (wzrost z 1,1 mld użytkowników w roku 2015 do 1,4 mld w roku 2020). Usługi oparte na lokalizacji będą najszybciej rosnącą konsumencką usługą mobilną (wzrost z 807 mln użytkowników w roku 2015 do 2,3 mld w roku 2020). Wideokonferencje będą najszybciej rosnącą usługą biznesową w internecie (wzrost z 95 mln użytkowników w roku 2015 do 248 mln w roku 2020);
- globalna ekspansja Wi-Fi – całkowita globalna liczba hotspotów Wi-Fi (publicznych i domowych) wzrośnie w latach 2015–2020 siedmiokrotnie, z 64 mln do 432 mln. Łącza Wi-Fi oraz komórkowe odpowiadać będą za 78% ruchu w sieciach IP w roku 2020 (Wi-Fi – 59%, komórkowe – 19%). Ruch w sieciach stacjonarnych stanowił będzie 22% całkowitego ruchu IP. W roku 2015 ruch w sieciach stacjonarnych stanowił 38% całego ruchu IP, w przypadku Wi-Fi było to 55%, zaś połączeń komórkowych – 7%.

Wideo dominuje

Ruch wideo w internecie wzrośnie czterokrotnie w latach 2015–2020, konsumencki ruch wideo będzie do roku 2020 stanowić 82% całkowitego konsumenckiego ruchu w internecie (wzrost z 68% w roku 2015), natomiast biznesowy ruch wideo będzie do roku 2020 stanowić 66% całkowitego biznesowego ruchu w internecie (wzrost z 44% w roku 2015).

Aktualna mapa połączeń transatlantyckich.

PROGNOZY DLA POLSKI

01 trzykrotny wzrost ruchu IP w latach 2015–2020, średnio o 25% rocznie;

02 sześciokrotny wzrost ruchu danych mobilnych w latach 2015–2020, średnio o 42% rocznie;

03 dane mobilne odpowiadały za 11% ruchu IP w roku 2015 i będą odpowiadać za 22% ruchu IP w roku 2020;

04 czterokrotny wzrost ruchu IP związanego z wideo w latach 2015–2020, średnio o 34% rocznie;

05 ruch związany z wideo (biznesowym i konsumenckim łącznie) będzie stanowił w roku 2020 70% całkowitego ruchu w internecie (wzrost z 49% w roku 2015). 75% tego ruchu będzie stanowić wideo w jakości HD, 9% w jakości ultra HD;

06 ruch związany z grami w internecie wzrośnie 7-krotnie i w roku 2020 będzie odpowiadał za 4% ruchu w Internecie konsumenckim;

07 w roku 2020 będzie 212,7 mln urządzeń podłączonych do sieci (wzrost z 125,5 mln w roku 2015). Oznacza to, że w roku 2020 na jednego mieszkańca będzie średnio przypadać 5,5 urządzenia. 42% wszystkich podłączonych urządzeń będą wówczas stanowić moduły M2M;

08 w roku 2020 komputery osobiste będą generować 34% ruchu IP (w roku 2015 było to 65%), ustępując miejsca smartfonom (39%) jako urządzeniom odpowiadającym za największą część polskiego ruchu IP. 17% generować będą tablety, 8% telewizory, a 2% moduły M2M;

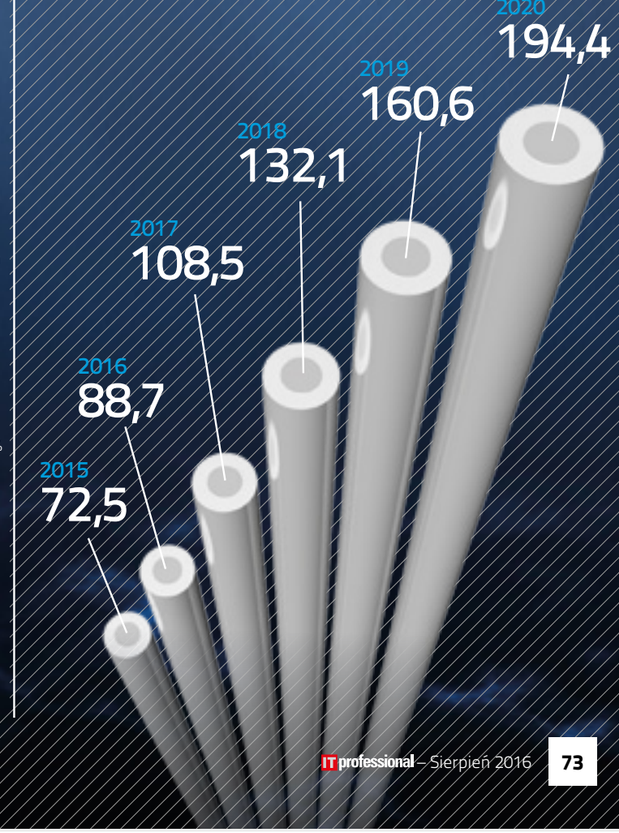
09 średnia szybkość stałych łączy internetowych wzrośnie w latach 2015–2020 ponad dwukrotnie, z 20,4 Mb/s do 42,3 Mb/s (w latach 2014–2015 średnia szybkość stałego łącza internetowego wzrosła w Polsce o 9%);

10 średnia szybkość łączy mobilnych wzrośnie pięciokrotnie i do roku 2020 osiągnie 12 Mb/s.

Dariusz Fabiszewski, dyrektor generalny Cisco w Polsce

Wraz z rozwojem cyfryzacji i podłączaniem do sieci coraz większej liczby ludzi i przedmiotów dane stają się najbardziej strategicznym zasobem firm, miast i państw. Umiejętność bezpiecznego wykorzystania danych do świadczenia nowych usług będzie determinować sukces. Wnioski z tegorocznego badania Cisco VNI wskazują na kilka wyraźnych trendów, jak wzrost znaczenia Internetu rzeczy i połączeń M2M. Kluczowa pozostaje także mobilność – tempo wzrostu ruchu danych w sieciach mobilnych będzie w naszym kraju dwukrotnie większe niż w stacjonarnych sieciach IP. Rozwijać będą się także zaawansowane usługi wideo i aplikacje M2M, napędzając zapotrzebowanie na większą przepustowość, szybkość i skalowalność sieci.

PROGNOZY ZAPOTRZEBOWANIA NA RUCH IP DO 2020 ROKU **[EB]**



ODNAWIALNE ŹRÓDŁA ENERGII

NIEZALEŻNOŚĆ ENERGETYCZNA?

Wykorzystanie odnawialnych źródeł energii (OZE) jest jednym z kluczowych działań polityki rozwojowej zarówno Polski, jak i Unii Europejskiej w zakresie ochrony klimatu, bezpieczeństwa energetycznego i ochrony środowiska. Ze względu na wysokie koszty budowy nowych elektrowni wykorzystujących OZE we wszystkich państwach tworzone są specjalne systemy wsparcia dla inwestorów. Jerzy Michalczyk

Przy ciągłych niepokojach na rynku energetycznym i malejących zasobach paliw kopalnych konieczna jest redukcja wykorzystania konwencjonalnych źródeł energii na rzecz energii uzyskiwanej ze źródeł odnawialnych. Odnawialne źródła energii to jeden z priorytetów polityki energetyczno-klimatycznej Unii Europejskiej. Jednym z jej celów jest 20-procentowy udział tych źródeł w finalnym zużyciu energii. Dla Polski ten cel jest nieco niższy – około 15,5%. Źródła odnawialne są jednak droższe od konwencjonalnych, ich rozwój trzeba więc wspierać poprzez dotacje.

Kwestie te kompleksowo reguluje ustawa z dnia 20 lutego 2015 r. o odnawialnych źródłach energii (DzU z 2015 r., poz. 478). Ustawa mówi m.in. o obowiązku zakupu energii i gwarantowanych taryfach na odsprzedaż energii elektrycznej przez tzw. prosumentów. Stała cena za prąd dotyczy energii ze źródeł do 3 kW i ma być stała przez 15 lat od oddania instalacji do użytku.

DOTACJE NA OZE

W latach 2014–2020 Polska będzie największym beneficjentem funduszy europejskich w ramach polityki spójności Unii Europejskiej – trafi do Polski w sumie ponad 80 mld euro. W tym okresie samorządy województw będą zarządzać około 40% tych środków. Zainwestują te pieniądze poprzez regionalne programy operacyjne. Duża część tych środków wiązać się będzie ze zwiększeniem efektywności energetycznej i rozwojem OZE. Unia Europejska przeznaczy w latach 2014–2020 – na ten cel w samych tylko 16 Regionalnych Programach Operacyjnych około 4,5 mld euro.

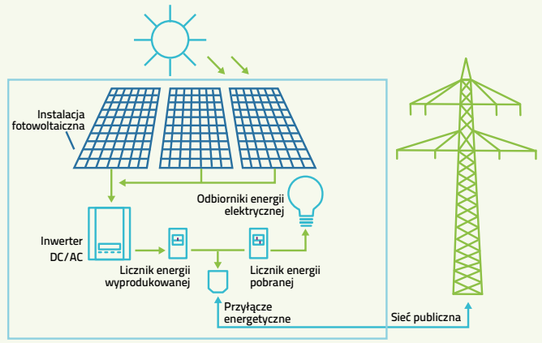
Programy Regionalne umożliwiają otrzymanie bezzwrotnych dotacji w wysokości 40–70% na realizację inwestycji w odnawialne źródła energii. Poziom pomocy będzie różny dla poszczególnych województw. Komisja Europejska określiła mapę pomocy regionalnej dla Polski z podziałem na województwa.

ILE KOSZTUJE INSTALACJA FOTOWOLTAICZNA

Na kompletną instalację fotowoltaiczną składają się elementy: panele fotowoltaiczne, inwerter, system mocowania, zabezpieczenia i przewody, a także koszty montażu i konfiguracji. Należy pamiętać, że w zależności od wielkości inwestycji ceny poszczególnych elementów będą stanowiły inny procent całości kosztów. **Przedstawiamy orientacyjną kalkulację dla przykładowej instalacji o mocy 10 kW.**

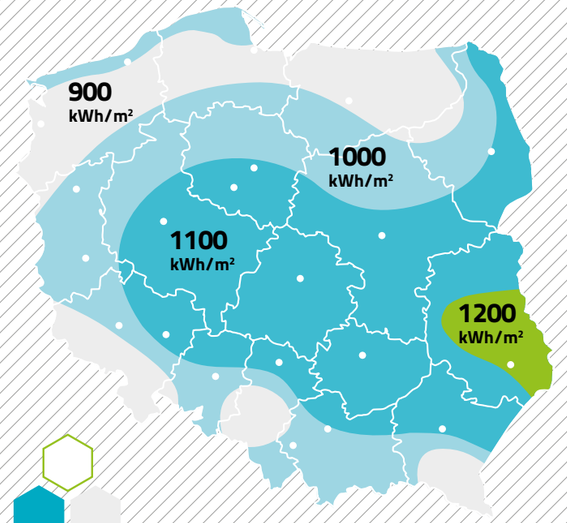
Elementy instalacji	Cena
Moduły fotowoltaiczne	32 000 zł
Inwerter	12 500 zł
System mocowania	5 000 zł
Zabezpieczenia i przewody	3 500 zł
Montaż	6 000 zł
Całkowity koszt inwestycji	**52 000 zł**
Cena za 1 kW	**5 200 zł**

SCHEMAT PROSTEJ INSTALACJI FOTOWOLTAICZNEJ W MAŁEJ FIRMIE LUB GOSPODARSTWIE DOMOWYM



Jednym ze źródeł energii jest energia słoneczna. Słońce jako źródło niewyczerpanej i najbardziej przyjaznej dla środowiska naturalnego energii odnawialnej staje się w dzisiejszych czasach niezwykle ważnym i niezawodnym dostawcą energii. Fotowoltaika to pozyskiwanie energii poprzez przetworzenie światła słonecznego na energię elektryczną w sposób bezpośredni, dzięki tzw. efektowi fotowoltaicznemu, który jest powszechnie wykorzystywany w modułach fotowoltaicznych. Produkowane obecnie moduły fotowoltaiczne cechują się sprawnością energetyczną sięgającą 14–16%. Producenci z reguły gwarantują, że sprawność ta w okresie 25 lat nie spadnie poniżej 80% początkowej wartości, zapewniają również gwarancję na wady utajone produktu do 10 lat. Inwerter jest urządzeniem elektronicznym, które steruje pracą systemu fotowoltaicznego. Najważniejszą funkcją inwertera jest zamiana prądu stałego wytwarzanego przez system fotowoltaiczny na prąd zmienny o parametrach umożliwiających zasilanie urządzeń elektrycznych, a także jego dostarczanie do sieci elektroenergetycznej. W mikroinstalacjach, tj. układach o mocy do 40 kW, zakład energetyczny wymienia na swój koszt obecny licznik energii na licznik dwukierunkowy, który umożliwia zliczanie energii zarówno wyprodukowanej, jak i zużytej przez budynek.

NASŁONECZNIENIE W POLSCE



FARMA FOTOWOLTAICZNA – ETAPY INWESTYCJI

1 LOKALIZACJA
Jednym z najistotniejszych działań, jakie należy podjąć, jest wybór odpowiedniej lokalizacji. Instalacja farmy fotowoltaicznej powinna być tak ustawiona, aby powierzchnia paneli była wystawiona na jak najdłuższe oddziaływanie słońca. Przyjmuje się, że w Polsce gęstość promieniowania słonecznego zawiera się w przedziale 900–1200 kWh/m², a ok. 80% z 1600 godzin całkowitej rocznej sumy nasłonecznienia przypada na okres wiosenno-letni.

2 PROJEKT INWESTYCJI
Uzyskanie warunków przyłączenia od lokalnego zakładu energetycznego wymaga złożenia stosownego wniosku. Konieczne jest sprecyzowanie parametrów instalacji oraz dołączenia specyfikacji urządzeń. Zgoda operatora będzie dotyczyć ściśle określonej konfiguracji, której nie można zmieniać na etapie realizacji.

3 POZWOLENIE NA BUDOWĘ I ZGŁOSZENIE INSTALACJI
Montaż urządzeń fotowoltaicznych o mocy elektrycznej do 40 kWp nie wymaga pozwolenia na budowę ani zgłoszenia. Jeśli jednak wysokość instalacji zainstalowanej na obiektach budowlanych przekracza 3 m, konieczne jest zgłoszenie budowy odpowiedniemu organowi.

4 KONCESJA
W przypadku inwestycji związanej z instalacją energetyczną konieczne jest uzyskanie koncesji. Kwestie te reguluje prawo energetyczne, określając wymagania, jakie obowiązują inwestorów występujących z wnioskiem do Urzędu Regulacji Energetyki (URE) o udzielenie takiej koncesji. Instalacje poniżej 5 MW zwolnione są z opłat za koncesję.

5 PRZYŁĄCZENIE DO SIECI I MONTAŻ INSTALACJI
Przed przyłączeniem instalacji do sieci elektrycznej konieczne jest określenie warunków przyłączenia. W tym celu należy złożyć odpowiedni wniosek do przedsiębiorstwa energetycznego, z którym chcemy nawiązać współpracę. Warunki przyłączenia wydawane są przez dystrybutora w ciągu 150 dni po złożeniu wniosku wraz z projektem umowy o przyłączenie do sieci i są ważne dwa lata. Podpisanie umowy następuje po uzgodnieniu i zatwierdzeniu danych złożonych we wniosku. Na zasadach określonych w danej umowie rozpoczyna się realizacja prac projektowych, budowlanych i montażowych. Za przyłączenie do sieci odpowiedzialny jest operator sieci.

6 MONTAŻ I INSTALACJA
Budowa instalacji fotowoltaicznej nie jest skomplikowana. Elektrownie fotowoltaiczne o mocy nawet kilku MW mogą być wykonane w ciągu miesiąca-dwóch, pod warunkiem właściwego zaplanowania dostaw i montażu podzespołów.

NOWE DOMENY, STARY SPAM

Nowy program rejestracji domen najwyższego poziomu uruchomiony w styczniu 2015 r. okazał się łakomym kąskiem dla spamerów. Dla cyberprzestępców nowe domeny stanowią narzędzie do promowania niechcianych lub nielegalnych kampanii reklamowych. Jerzy Michalczyk

Nowa paleta domen najwyższego poziomu (gTLD – generic top-level domain) pozwala wybrać strefę domen odpowiadającą działalności organizacji oraz tematyce jej stron internetowych. Na przykład serwisy związane z pracą mogą teraz wykorzystywać domenę .work a strony naukowe mogą znaleźć się w domenie .science. Ze względu na możliwości, jakie daje nowy program gTLD, został on entuzjastycznie przyjęty przez społeczność internetową i obecnie obserwujemy aktywną rejestrację nowych nazw domen. Na ten trend równie szybko zareagowali jednak także spamerzy i cyberprzestępcy. Na skutek ich działalności nowe strefy domen niemal natychmiast stały się areną dystrybucji spamu reklamowego, wiadomości phishingowych oraz zawierających szkodliwe programy – tak wynika z analizy przeprowadzonej przez Kaspersky Lab w pierwszym kwartale 2015 r. Z obserwacji ruchu e-mail wynika, że w pierwszym kwartale 2015 r. nastąpił znaczny wzrost liczby nowych domen rozsyłających treści spamowe, chociaż odsetek spamu w porównaniu z poprzednim kwartałem zmniejszył się.

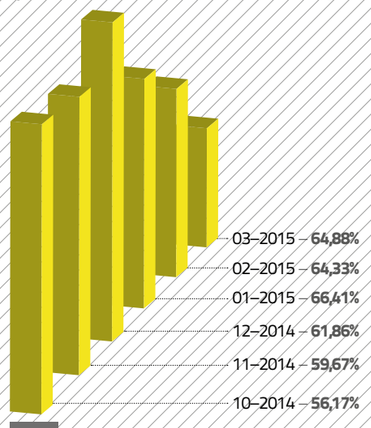
W pierwszym kwartale ruch spamowy zawierał również wiele e-maili wysyłanych z domen takich jak .pink .red czy .black. Były one często wykorzystywane w celu reklamowania azjatyckich portali randkowych.

Ruch spamowy w pierwszym kwartale 2015 r. zawierał dużą liczbę masowych wysyłek z załącznikami Microsoft Word lub Excel, które kryły makrowirusy. Oszuści próbowali skłonić użytkowników do otwarcia szkodliwych plików poprzez zamaskowanie ich pod postacią różnych dokumentów, w tym finansowych. Fałszywe wiadomości często imitowały powiadomienia od dobrze znanych organizacji oraz serwisów. Trzy czołowe źródła spamu wysyłanego na całym świecie to Stany Zjednoczone (14,5%), Rosja (7,27%) oraz Ukraina (5,56%). Na pierwszym miejscu rankingu państw stanowiących najczęstszy cel masowych wysyłek znalazła się Wielka Brytania (w której odsetek wiadomości rekla-

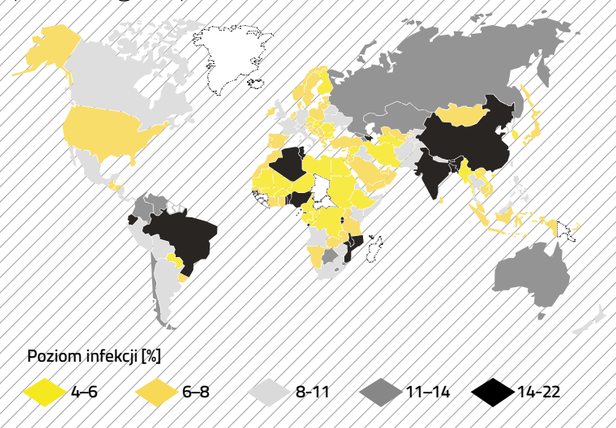
mujących stanowił 7,85% wszystkich wykryć szkodliwego oprogramowania w wiadomościach e-mail).

Jeśli chodzi o kategorie spamu, jeden z najpopularniejszych tematów stanowiły ubezpieczenia, zarówno pod względem liczby wiadomości, jak i liczby zmieniających się domen widocznych w masowych wysyłkach. Spam oferujący usługi ubezpieczeniowe wykorzystywał nowo utworzone domeny najwyższego poziomu, jak również takie, które zostały zhakowane lub wygasła ich ważność. Nawet jeśli domeny były nowe, spamerzy nadal stosowali stare sztuczki, na przykład podmieniali domeny znanych organizacji, takie jak @amazon.com czy @ebay.com w polu „Od".

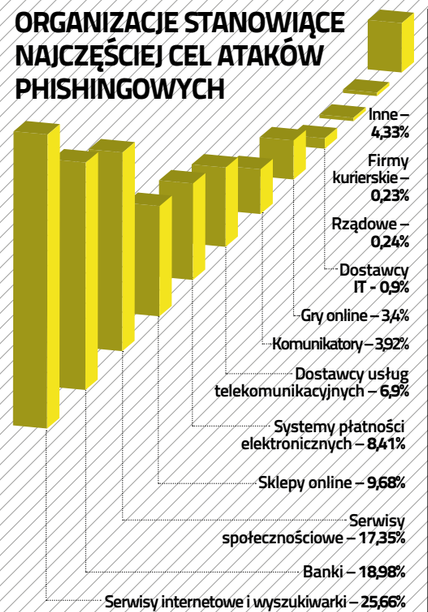
Spam w ruchu e-mail
(październik 2014 – marzec 2015)



Rozkład geograficzny ataków phishingowych



ORGANIZACJE STANOWIĄCE NAJCZĘŚCIEJ CEL ATAKÓW PHISHINGOWYCH



Analiza ogólnych danych dla pierwszego kwartału oraz informacji dotyczących rodzaju spamu w nowych domenach pokazuje, że jednym z najpopularniejszych tematów pod względem liczby wiadomości oraz liczby zmieniających się domen w masowych wysyłkach była działalność ubezpieczeniowa. Spam ten dotyczył wszystkich typów ubezpieczenia – na życie, zdrowotnego, mienia, pojazdów, zwierząt oraz na wypadek pogrzebu.

Tatiana Szczerbakowa, starszy analityk spamu, Kaspersky Lab

ŹRÓDŁO: KASPERSKY LAB

Phishing

Największy odsetek użytkowników dotkniętych atakami phishingowymi znajdował się w Brazylii, chociaż w pierwszym kwartale 2015 r. liczba ta (18,28%) zmniejszyła się o 2,74 punktu procentowego.

W rankingu organizacji najczęściej atakowanych przez phisherów w trzecim kwartale 2014 kategoria „serwisy e-mail i wyszukiwarki" odnotowała znaczny spadek, nadal jednak zajmuje najwyższe miejsce (25,66%) w rankingu dla 2015 r. Pojawiła się też nowa kategoria – „firmy kurierskie". Jej udział obecnie jest niewielki (jedynie 0,23%), ale to nowy trend, o którym warto wspomnieć. Oszuści w wiadomościach e-mail oferują nabycie towarów z dostawą realizowaną przez znaną firmę logistyczną. Jeśli odbiorca się zgodzi, wymagają zapłaty za wysyłkę z góry i dostarczają fałszywe faktury z logo danego kuriera. Po otrzymaniu pieniędzy oszuści znikają.

Wiadomości phishingowe wysyłane w imieniu firm logistycznych często zawierają szkodliwe załączniki. Zwykle e-mail zawiera powiadomienie o dostawie; aby odebrać towar, odbiorca musi otworzyć załącznik, który okazuje się szkodliwy, lub odwiedzić stronę internetową i umieścić na niej swoje dane osobiste. Ta druga metoda jest wykorzystywana do zbierania aktywnych adresów e-mail oraz innych informacji osobistych użytkowników.

Jak wynika z rankingu Kaspersky Lab, najczęściej rozprzestrzenianym za pośrednictwem poczty elektronicznej szkodliwym oprogramowaniem był Trojan-Banker.Win32.ChePro.ink. Z kolei downloadery z rodziny Upatre, które służą do pobierania trojana bankowego Dyre/Dyreza, stały się najpopularniejszą rodziną szkodliwego oprogramowania w badanym okresie.

SPAM I PHISHING W PIERWSZYM KWARTALE 2015 r.

Odsetek spamu w ruchu e-mail, według danych obejmujących pierwszy kwartał 2015 r., wynosił 59,2% - co stanowi spadek o 6 punktów procentowych w stosunku do poprzedniego kwartału.

Stany Zjednoczone utrzymały pozycję największego źródła spamu, wysyłając 14,5% niechcianych wiadomości.

Phishing skierowany przeciwko klientom organizacji finansowych stanowił 37,06% wszystkich zarejestrowanych incydentów.

50 077 057

przypadków ataków phishingowych zarejestrowały produkty firmy Kaspersky Lab. Jest to o 1 milion więcej niż w poprzednim kwartale.

IBM LinuxONE

WYDAJNE SERWERY PLUS ZESTAW OTWARTYCH APLIKACJI

LinuxONE to zestaw zintegrowanych rozwiązań stworzony z myślą o średnich i dużych przedsiębiorstwach, obejmujący sprzęt, oprogramowanie i usługi. W jego skład wchodzą m.in. wydajne serwery LinuxONE Emperor i LinuxONE Rockhopper oraz otwarte środowisko programistyczne DeveloperCloud z dostępem do ApacheSpark.

Sebastian Kuniszewski

LinuxONE firmy IBM to nowe, bezpieczne i wydajne rozwiązania zaprojektowane z myślą o analityce biznesowej i działaniu w środowisku chmur hybrydowych. Łączy w sobie wydajne serwery mainframe, dedykowany zestaw otwartych aplikacji i narzędzi branżowych oraz możliwości udostępnionej przez IBM chmury dla deweloperów i kodów źródłowych oprogramowania. Całe rozwiązanie pozwala na kompleksową obsługę procesów biznesowych, możliwość elastycznego wykorzystania technologii wirtualizacyjnych i sprawne tworzenie nowych aplikacji. – Piętnaście lat temu IBM rozpoczął wprowadzanie Linuksa na swoje serwery mainframe, a dziś korzysta z nich co trzeci klient firmy stosujący maszyny tej klasy – mówi Maciej Gruczyński z IBM. – Jednocześnie zwiększamy nasze zaangażowanie w obszarze otwartych rozwiązań, łącząc najlepsze oprogramowanie z najbardziej zaawansowanym sprzętem. Umożliwia to obsługę systemów mobilnych i chmur hybrydowych. Dzięki stosowaniu Linuksa na serwerach mainframe uzyskujemy możliwości znacznie przekraczające te, które oferują powszechnie stosowane architektury serwerowe, zwłaszcza jeśli chodzi o bezpieczeństwo i moc obliczeniową – dodaje.

ZAAWANSOWANA PLATFORMA KLASY ENTERPRISE

W skład LinuxONE wchodzą dwa systemy, którym nadano nazwy gatunków pingwinów. Pierwszy z nich – **LinuxONE Emperor** wykorzystuje serwery IBM z13. Dzięki zastosowaniu nowych, wyjątkowo wydajnych procesorów (patrz ramka obok) jest to jeden z najbardziej zaawansowanych systemów Linux na świecie, który może analizować transakcje w czasie rzeczywistym i zapobiegać na bieżąco wykrywanym oszustwom. System jest skalowalny do 8 tysięcy maszyn wirtualnych lub tysięcy kontenerów. Z kolei **LinuxONE Rockhopper** wyposażony w starsze procesory z12 jest rozwiązaniem dla klientów, którym zależy na szybkości, bezpieczeństwie i niezawodności działania serwera, ale mają oni nieco mniejsze potrzeby niż duże korporacje i ograniczone zasoby. Jak zapewnia IBM, oba serwery oferują niemal nieograniczoną skalowalność oraz zaawansowane możliwości szyfrowania

Jeden system z13 może zawierać do 141 procesorów, wytwarzanych w technologii 22 nm, które mają 8 rdzeni i są taktowane zegarem o częstotliwości 5 GHz. Administrator może w systemie skonfigurować do 8 tys. maszyn wirtualnych.

LinuxONE Emperor

zarówno w warstwie sprzętowej, jak i oprogramowania (zwiększone bezpieczeństwo w porównaniu do rozwiązań wyposażonych w klucze nieszyfrowane oraz do 28 razy większą wydajność niż standardowe technologie z kluczami szyfrowanymi).

OTWARTE OPROGRAMOWANIE DLA SYSTEMÓW

Nowe serwery LinuxONE mogą w pełni wykorzystywać możliwości popularnych otwartych środowisk, aplikacji i narzędzi branżowych, takich jak Apache Spark, Node.js, MongoDB, MariaDB, PostgreSQL i Chef, oraz zapewniają wirtualizację zasobów dzięki zgodności z hipernadzorcami KVM i SUSE. Producent stworzył też chmurę LinuxONE Developer Cloud, która funkcjonuje jako wirtualny silnik R&D umożliwiający tworzenie, testowanie i wdrażanie aplikacji, w tym mobilnych i działających w chmurach hybrydowych. Dodatkowo Canonical planuje udostępnić skalowalną dystrybucję Ubuntu dla LinuxONE oraz IBM System Z, a firma IBM przystąpiła do realizowanego przez Linux Foundation projektu Open Mainframe, jednocześnie udostępniając społeczności open source około pół miliona linii kodu. W głównej mierze pochodzi on z oprogramowania do analityki predykcyjnej i pozwala deweloperom na rozwój własnych aplikacji. Inicjatywa Open Mainframe Project zrzesza producentów i ekspertów z branży w celu wspierania innowacji i rozwoju Linuksa na platformie mainframe, a firmy partycypujące będą razem budować narzędzia i technologie open source dla systemów mainframe.

Więcej informacji:
ibm.com/linuxone

LinuxONE Emperor (IBM z13) w pigułce

- **2,5 miliarda chronionych transakcji dziennie. Według szacunków do 2025 r. wykonywanych będzie 40 bilionów transakcji mobilnych w ciągu dnia;**
- **Podwojona prędkość szyfrowania danych w czasie rzeczywistym, umożliwiająca szybsze i bezpieczniejsze wykonywanie operacji finansowych;**
- **Opatentowane szyfrowanie kryptograficzne, gwarantujące większe bezpieczeństwo transakcji na urządzeniach mobilnych;**
- **Wbudowane narzędzia analityczne, zapewniające wgląd w transakcje mobilne w czasie rzeczywistym i działające 17 razy szybciej niż jakakolwiek dotychczas dostępna technologia.**

CHMURY I USŁUGI MOBILNE

JIM ZEMLIN
dyrektor wykonawczy
Linux Foundation

Usługi mobilne i chmury obliczeniowe stają się wszechobecne, a to wymaga, aby organizacje mogły jak najbardziej efektywnie i wydajnie przetwarzać gromadzone dane. Linux na komputerach typu mainframe właśnie takie rozwiązania dostarcza. Co ważne, prowadzony przez Linux Foundation projekt Open Mainframe skupia technologicznych liderów, którzy wspólnie pracują nad rozwojem Linuksa i zaawansowanymi technologiami dla całej branży IT i środowisk akademickich. Wszystko po to, aby zaprojektowane przez nich rozwiązania mogły obsługiwać i jak najefektywnie j przetwarzać nawet najbardziej skomplikowane zadania stawiane przed nowoczesnymi systemami IT.

LinuxONE Rockhopper

IMPONUJĄCE MOŻLIWOŚCI IBM z13

Na początku 2015 r., niemal trzy lata po premierze systemu mainframe z12, IBM zaprezentował platformę z13 – wydajne rozwiązanie oparte na nowym procesorze i mogące zarządzać trzy razy większą pamięcią niż z12 (do 10 TB). Jeden system z13 może zawierać do 141 procesorów, a administrator może na nim skonfigurować do 8 tys. wirtualnych maszyn. Procesory instalowane w z13 mają osiem rdzeni i są taktowane zegarem o częstotliwości do 5 GHz. Co ważne, mogą one wykonywać podczas jednego taktu zegara dwie instrukcje (praca w trybie SMP) oraz wspierają technologie SIMD (Single Instruction, Multiple Data) i DB2 BLU for Linux (obsługują bazy danych typu in-memory). Zdaniem producenta platforma IBM z13 to pierwszy system mainframe zdolny przetwarzać dziennie 2,5 miliarda operacji, jednocześnie szyfrując transakcje w czasie rzeczywistym. Rozwiązanie ma również wbudowane mechanizmy analityczne ułatwiające bieżącą analizę transakcji. Ich wydajność jest do 17 razy większa niż w przypadku rozwiązań konkurencyjnych. Pozwala to na „szybsze wykrywanie nadużyć i prowadzone w czasie rzeczywistym monitorowanie zachowań klientów oraz podejmowanie dodatkowych działań sprzedażowych jeszcze w trakcie trwania transakcji". Dodatkowo platforma IBM z13 charakteryzuje się nawet dwukrotnie wyższą szybkością szyfrowania danych w porównaniu do maszyn poprzedniej generacji. Wykorzystano przy tym opatentowane mechanizmy szyfrowania kryptograficznego. Zdaniem przedstawicieli IBM ta funkcjonalność „pomoże zapobiegać nadużyciom finansowym już w chwili ich wykonywania, umożliwiając instytucjom finansowym wstrzymanie transakcji, zanim konsument zostanie poszkodowany".

05. *ABI Expert* magazine

ABI Expert is a quarterly dedicated to the issues of personal data protection as well as legal and practical issues of information administration. The magazine is intended for data protection officers, data controllers as well as persons responsible for the organization of the personal data protection system, as well as supervision over their processing and security. The quarterly is of an expert nature, but the issues raised in its pages are presented in an accessible way and relate to the practice of applying the regulations and technical solutions ensuring the security of data processing.

Scope of work:
– design
– layout
– typography
– desktop publishing
– pre-press

Cover by Krzysztof Kanoniak

↑ Click to move to Table of Contents

ABI-EXPERT.PL

ABI EXPERT

Prawne i techniczne aspekty ochrony danych i informacji

1 2017

nr 1 (2) styczeń–marzec 2017

10

Zgoda na przetwarzanie danych osobowych

Skuteczne wyrażenie zgody, kiedy jej żądać oraz jakie warunki musi spełniać zgoda na przetwarzanie danych osobowych?

ISSN 2451-3970

Cena 68,00 zł (w tym 5% VAT)

ABI EXPERT

ADRES REDAKCJI
ul. Krakowska 29
50-424 Wrocław
tel. 71 797 28 46
faks 71 797 28 16

ADRES INTERNETOWY
www.abi-expert.pl
redakcja@abi-expert.pl

REDAKTOR NACZELNA
dr Marlena Sakowska-Baryła
marlena.sakowska@abi-expert.pl

SEKRETARZ REDAKCJI
Paulina Skoczylas
paulina.skoczylas@abi-expert.pl

RADA PROGRAMOWA
Artur Cieślik, dr hab. Paweł Fajgielski, r.pr. dr hab. Bogdan Fischer, adw. Xawery Konarski, r.pr. Andrzej Lewiński, adw. dr Paweł Litwiński, r.pr. dr Arwid Mednis, dr Arleta Nerka, dr Agnieszka Piskorz-Ryń, adw. dr Grzegorz Sibiga, r.pr. Daniel Ślęzak, Mariola Więckowska

KOREKTA
Bogusława Otfinowska

PROJEKT GRAFICZNY I SKŁAD
Marcin Szewczyk
dtp@presscom.pl

WYDAWCA
PRESSCOM Sp. z o.o.
ul. Krakowska 29
50-424 Wrocław
www.presscom.pl
biuro@presscom.pl

PREZES ZARZĄDU
Paweł Podkański

DYREKTOR WYDAWNICZY
Przemysław Golis

REKLAMA
Mikołaj Marzec
tel. 71 797 48 05 / tel. kom. 606 792 942
mikolaj.marzec@presscom.pl

Alina Merchelska
tel. kom. 604 174 172
alina.merchelska@presscom.pl

Patrycja Kubiak-Rogalna
tel. kom. 728 980 807
patrycja.kubiak@presscom.pl

PATRONATY
Jacek Śmieszek-Świętalski
tel. 71 797 28 30
jacek.smieszek@presscom.pl

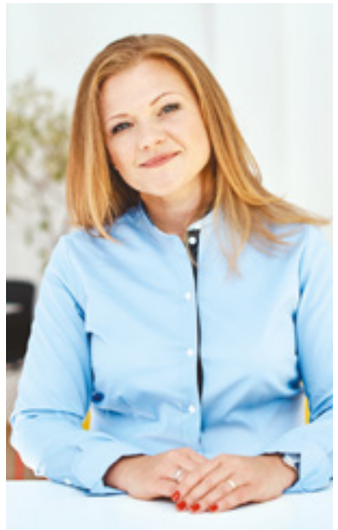
PRENUMERATA
tel. 71 797 28 34
prenumerata@abi-expert.pl
www.abi-expert.pl

Santander Bank Polska S.A.
96 1090 1522 0000 0001 0162 2418

Nakład 4000 egz.

Okładka
Krzysztof Kanoniak

Wydawca jest członkiem Izby Wydawców Prasy



Marlena Sakowska-Baryła

dr Marlena Sakowska-Baryła
redaktor naczelna

KONTROLE I OŚWIATA

W ielu inspektorów ochrony danych powszechnie dzieli się przeświadczeniem, że 2019 rok upłynie pod znakiem weryfikacji wdrożeniowych zmagań z rodo, która następować będzie poprzez zapowiadane kontrole Prezesa Urzędu Ochrony Danych Osobowych. Zapewne jest w tym twierdzeniu sporo prawdy, skoro zapowiedzi owych kontroli płyną z samego Urzędu. Dlatego też, wychodząc naprzeciw potrzebom, oczekiwaniom i obawom, w bieżącym numerze kontrolą przez UODO zajmujemy się bliżej, otwierając tym samym cykl artykułów poświęconych tej tematyce, krok po kroku tłumacząc zagadnienia z zakresu postępowania kontrolnego, a następnie postępowania przed organem nadzorczym i sądami administracyjnymi – tak na wszelki wypadek, gdyby rzeczona weryfikacja nie wypadła za bardzo pomyślnie.

Innym aspektem o charakterze quasi-kontrolnym pozostają relacje administratorów z organami ochrony prawnej, które z mocy prawa mogą żądać od nich różnego rodzaju danych osobowych. Mierzymy się z tym zagadnieniem, publikując zestawienie przypadków, gdy służby mogą żądać danych od przedsiębiorców telekomunikacyjnych.

Inspiracji do przyjrzenia się naszym działaniom i zrewidowania przekonań odnośnie do tego, co jest, a co nie jest zgodne z rodo, chcemy dostarczyć także poprzez poświęcenie szerszej uwagi ochronie danych osobowych w oświacie. Wydaje się, że tam jak w soczewce szczególnie intensywnie skupiły się i absurdy, i problemy stosowania przepisów o ochronie danych osobowych. Stosujmy je zatem tak, by chronić osobę fizyczną – jej prywatność, godność i interesy, nie zaś dane osobowe dla samych danych, bo „numerowanie" uczniów nic tu nie załatwia, a bywa groteskowe.

RELACJA

3–4 KWIETNIA 2017 R. – HOTEL SOBIENIE KRÓLEWSKIE GOLF & COUNTRY CLUB K. WARSZAWY

FORUM ADMINISTRATORÓW BEZPIECZEŃSTWA INFORMACJI

Forum Administratorów Bezpieczeństwa Informacji to ogólnopolska Konferencja przygotowana dla osób odpowiedzialnych za organizację systemu ochrony danych osobowych oraz nadzór nad ich przetwarzaniem i zabezpieczaniem. Organizatorem wydarzenia był wydawca Kwartalnika „ABI Expert".

Celem spotkania było przygotowanie do wdrożenia unijnych przepisów ogólnego rozporządzenia o ochronie danych osobowych (rodo), które zaczną być stosowane od 25 maja 2018 r. Uczestnicy Konferencji dowiedzieli się m.in.:

- jak wyznaczyć IOD na tle wytycznych Grupy Roboczej Art. 29;
- czym jest prawo do przenoszenia danych i jakie problemy praktyczne może sprawiać jego realizacja;
- czym jest ochrona danych w fazie projektowania (*privacy by design*);
- jak realizować prawo do bycia zapomnianym oraz obowiązek zgłaszania naruszeń ochrony danych organowi nadzorczemu;
- jak zabezpieczyć systemy teleinformatyczne w zgodzie z przepisami rodo;
- które dane osobowe pracowników mogą, a które nie mogą być udostępniane;
- jak przygotować dokumentację przetwarzania danych osobowych;
- OSOD – Krok po Kroku.

Główny nacisk podczas poszczególnych prelekcji został położony na praktyczny aspekt realizacji przepisów rodo. Redaktor naczelna kwartalnika „ABI Expert" Marlena Sakowska-Baryła wprowadziła w tematykę forum: „Jesteśmy w momencie historycznym, bodaj najciekawszym momencie organizacji systemu ochrony danych osobowych w naszym kraju i w Unii Europejskiej. Mamy rozporządzenie ogólne, znamy już te przepisy, będziemy starali się dzisiaj przełożyć język prawniczy na język praktyki. Czasu pozostało niewiele do tego, żeby rozpocząć stosowanie przepisów w pełnym zakresie. **Obowiązków z pewnością mamy coraz więcej. Kilka dni temu pojawiły się założenia do projektu ustawy o ochronie danych osobowych**. Te przepisy także będą wymagały szerszej rozwagi, szerszego omówienia. Nasze dzisiejsze spotkanie, podczas którego będziemy mieli okazję usłyszeć wielu znamienitych ekspertów, ale również praktyków w zakresie ochrony danych osobowych, pozwoli nam przybliżyć te zagadnienia. Myślę, że zarówno w tej części bardziej oficjalnej, kiedy będziemy rozważać poszczególne zagadnienia związane z rodo, jak i w czasie naszych mniej oficjalnych, kuluarowych spotkań będziemy mogli o tych wszystkich zagadnieniach porozmawiać".

Więcej zdjęć oraz informacji o prelegentach na stronie: **www.forum.abi-expert.pl**

PRELEGENCI

Roman Bieda – radca prawny i rzecznik patentowy

Artur Cieślik – redaktor naczelny „IT Professional"

Michał Czerniawski – specjalista w zakresie prawa ochrony danych osobowych

Agnieszka Gryszczyńska – doktor nauk prawnych

Anna Kobylańska – specjalista w zakresie prawa własności intelektualnej, nowych technologii i ochrony danych osobowych

Arwid Mednis – specjalista w zakresie prawa telekomunikacyjnego

Arleta Nerka – specjalista w zakresie prawa ochrony danych osobowych, prawie pracy i ubezpieczeń społecznych

Marlena Sakowska-Baryła – redaktor naczelna „ABI Expert"

Piotr Siemieniak – zajmuje się ochroną danych osobowych i tworzeniem oprogramowania

Łukasz Ślęzak – specjalizuje się w realizacji projektów dotyczących bezpieczeństwa informacji i danych osobowych

Mariola Więckowska – ABI w Grupie Allegro, Ceneo i Naspers Classifieds

Krzysztof Wygoda – doktor prawa.

Fot. Paweł Konarzewski

B ALFABET ODO

Biometria, dane biometryczne – według rodo dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, np. wizerunek twarzy (zdjęcie, fotografia) lub dane daktyloskopijne (linie papilarne, odcisk palca). Dane biometryczne należą do kategorii danych szczególnie chronionych, tzw. wrażliwych. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych biometrycznych. Przetwarzanie zdjęcia, fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Generalny Inspektor Ochrony Danych Osobowych uznał za niedopuszczalne wykorzystywanie przez pracodawców danych biometrycznych pracowników do kontroli czasu pracy. Takie samo stanowisko zostało wyrażone przez sądy. Grupa Robocza Art. 29 wydała kilka opinii na temat przetwarzania danych biometrycznych zarówno w sektorze państwowym, jak i prywatnym, ze szczególnym wskazaniem na warunki techniczne przetwarzania i właściwego zabezpieczenia biometrii.

Bezpieczeństwo – przepisy rodo mają na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, postępu społeczno-gospodarczego, wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także pomyślności ludzi (motyw 2 rodo). W preambule prawodawca posługuje się takimi stwierdzeniami, jak bezpieczeństwo narodowe, publiczne sieci i informacji, bezpieczeństwo usług, przetwarzania, poziomy i środki bezpieczeństwa. Zgodnie z art. 32 rodo „Bezpieczeństwo przetwarzania", administrator danych i podmiot przetwarzający (procesor) są zobowiązani wdrożyć środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa, odpowiadający m.in. ryzyku przetwarzania danych w organizacji.

Anna Buczyńska-Borowy – autorka jest ABI, audytorem, Konsultantem, prowadzi szkolenia w zakresie ochrony danych osobowych.

DANE Z KRS – CZY MOŻNA OGRANICZYĆ DO NICH DOSTĘP?

Polskie przepisy zabraniają Korzystania z prawa do bycia zapomnianym wobec rejestrów handlowych, takich jak Krajowy Rejestr Sądowy, i jako takie są zgodne z najnowszym wyrokiem Trybunału Sprawiedliwości UE. Czy dane z takich rejestrów mogą być w Polsce przedmiotem ograniczeń w dostępie, którą to decyzję TSUE pozostawił sądom krajowym?

9 marca 2017 r. TSUE wydał wyrok dotyczący możliwości anonimizacji danych o upadłości spółki figurujących w rejestrze spółek – sprawa Manni (C-398/15). Sprawa Manni dotyczyła obywatela Włoch, który domagał się usunięcia z włoskiego rejestru spółek informacji o tym, że pełnił funkcję zarządzającego i likwidatora jednej ze spółek. Spółka ta ogłosiła upadłość w 1992 r. i została usunięta z rejestru spółek w 1995 r. Wskazywał, że informacja co do upadłej spółki utrudnia mu prowadzenie obecnej działalności, i żądał od izby handlowej prowadzącej rejestr wykreślenia, anonimizacji lub zablokowania danych łączących jego nazwisko z upadłością spółki oraz zasądzenia od izby handlowej zapłaty odszkodowania za wyrządzoną szkodę wizerunkową. Sąd pierwszej instancji przychylił się do jego żądań. Więcej wątpliwości miał włoski trybunał kasacyjny, który zawiesił postępowanie i skierował pytania dotyczące tej sprawy do TSUE.

TSUE wskazał, że dyrektywa 68/151 dotycząca zapewnienia ochrony interesów zarówno wspólników, jak i osób trzecich ma na celu w szczególności ochronę interesów osób trzecich w stosunkach ze spółkami akcyjnymi i spółkami z ograniczoną odpowiedzialnością, gdyż jedyną gwarancją, jaką te podmioty oferują osobom trzecim, jest majątek spółki. Podstawowe dokumenty spółki powinny być jawne, aby umożliwić osobom trzecim zapoznanie się z ich treścią oraz innymi informacjami dotyczącymi danej spółki, w szczególności z danymi osób, które są uprawnione do nabywania praw i zaciągania zobowiązań w jej imieniu.

TSUE wprost odrzuca możliwość usunięcia bądź anonimizacji danych z rejestru handlowego, natomiast w zakresie ograniczenia do nich dostępu osobom trzecim odsyła do prawa krajowego i przerzuca ciężar oceny poszczególnych stanów faktycznych na sądy krajowe.

Polski KRS korzysta z domniemania prawdziwości i aktualności zawartych w nim informacji. Jednym z filarów jego funkcjonowania jest zaufanie obywateli do poprawności treści dokonywanych w nim wpisów, które co do zasady podlegają ogłoszeniu w oficjalnym państwowym publikatorze, jakim jest Monitor Sądowy i Gospodarczy. Jednocześnie w prawie polskim obowiązuje zasada zakazu usuwania informacji z KRS. Zgodnie z art. 12 ust. 1 ustawy o Krajowym Rejestrze Sądowym dane zawarte w rejestrze nie mogą być z niego usunięte, chyba że ustawa stanowi inaczej. Natomiast zgodnie z art. 34 ust. 1 ustawy o swobodzie działalności gospodarczej dane zawarte w CEIDG nie mogą być z niej usunięte, chyba że ustawa stanowi inaczej. Samo wykreślenie wpisu w CEIDG nie oznacza usunięcia danych, a ewidencja ta umożliwia wyszukiwanie informacji o podmiotach z niej wykreślonych.

ZATRZYMYWANIE DANYCH

21 grudnia 2016 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawach połączonych C-203/15 Tele2 Sverige AB/ Post-ochtelestyrelsen i C-698/15 Secretary of State for the Home Department/Tom Watson i in., w którym stwierdził, że państwa członkowskie nie mogą nakładać na operatorów telekomunikacyjnych ogólnego obowiązku zatrzymywania danych.
Prawo UE zabrania masowego zatrzymywania wszystkich danych dotyczących ruchu w sieci i lokalizacji. Państwa członkowskie mają jednak możliwość wprowadzenia przepisów prawa, które pozwalają na retencję niektórych danych w celu zwalczania poważnej przestępczości.
Taki dostęp może zostać przyznany jedynie odnośnie do danych dotyczących osób podejrzewanych o planowanie, popełnianie czy też dopuszczenie się poważnego przestępstwa lub zaangażowanych w przestępstwo. Trybunał uznał ponadto za istotne, aby dostęp do przechowywanych danych podlegał wcześniejszej kontroli sprawowanej przez sąd lub inny niezależny organ. Przepisy krajowe powinny ustanawiać obowiązek przechowywania danych na obszarze UE, a także obowiązek ich nieodwracalnego niszczenia po upływie okresu ich przechowywania.

OŚWIADCZENIA ZAMIAST ZAŚWIADCZEŃ

16 stycznia Ministerstwo Rodziny Pracy i Polityki Społecznej (dalej: MRPiPS) we współpracy z Ministerstwem Cyfryzacji uruchomiło cztery w pełni scyfryzowane usługi, dzięki którym można składać wnioski m.in. o becikowe, świadczenie z Funduszu Alimentacyjnego czy Kartę Dużej Rodziny.

To kolejny etap w realizacji cyfrowej rewolucji, której efektem ma być urząd dostępny dla obywateli 24 godziny na dobę przez 7 dni w tygodniu. W usługach online, które uruchomiło właśnie MRPiPS, dane, przynajmniej częściowo, same zaciągają się do wniosków. Uruchomienie tych usług oznacza, że ok. pół miliona osób rocznie (nie licząc tych, którzy składają wnioski o wypłatę 500+) nie będzie musiało iść do urzędu, by dostać np. becikowe. Żeby skorzystać z tej możliwości, wystarczy mieć Profil Zaufany (eGO) – darmowy podpis elektroniczny, który wystarcza do załatwiania online spraw urzędowych.

Od października z takiej możliwości skorzystało już ponad 60 tys. osób. Profil Zaufany można uzyskać teraz w trzech dużych bankach (PKO BP, ING, Millennium) – to już ok. 35% rynku.

PUBLIKACJA ORZECZEŃ TK W BIP

Publikowane w BIP orzeczenia Trybunału Konstytucyjnego muszą być bezwzględnie anonimizowane – uznał WSA w Warszawie w wyroku z 19 stycznia 2017 r. (II SA/Wa 1434/16), przyznając tym samym rację GIODO.

Zagadnieniem tym GIODO zajmował się w związku ze skargą osoby, której dane osobowe – jako osoby inicjującej postępowanie przed TK – zostały upublicznione w BIP Trybunału w związku z publikacją orzeczenia wydanego w zgłoszonej przez nią sprawie.

Zdaniem GIODO, publikacja orzeczenia TK w BIP po poddaniu go anonimizacji, tj. po usunięciu z jego treści informacji identyfikujących osobę fizyczną, pozwala wszystkim zainteresowanym na poznanie treści takiego orzeczenia. Mimo spełnionych w ten sposób warunków dostępności i powszechnej znajomości opublikowanego orzeczenia zostaje zachowane prawo do prywatności osób, których dotyczy.

W przypadku publikowania treści orzeczenia w Dzienniku Ustaw, imię i nazwisko osoby inicjującej postępowanie przed TK publikowane są w całości, bez poddawania orzeczenia anonimizacji. Nie ma to znaczenia dla tego wyroku, ponieważ należy odróżnić publikację danych osobowych osoby składającej skargę w Dzienniku Ustaw od publikacji jej danych w BIP Trybunału.

CETA A OCHRONA DANYCH

Ministerstwo Cyfryzacji wprowadziło do kompleksowej umowy gospodarczo-handlowej między Unią Europejską a Kanadą (CETA) postanowienia interpretacyjne pozwalające zabezpieczyć interes państw członkowskich w obszarze ochrony prywatności oraz ochrony danych osobowych w kontekście handlu elektronicznego i przepływu danych, w tym danych osobowych.
Z perspektywy Unii Europejskiej najważniejsze kwestie to:

- głęboka liberalizacja dostępu do rynków usług,
- zapewnienie swobody działania,
- niedyskryminowanie inwestorów.

30 października 2016 r. po trwających 5 lat negocjacji podpisano umowę na szczycie Unia Europejska–Kanada. W imieniu Polski i pozostałych państw członkowskich Unii Europejskiej negocjacje prowadziła Komisja Europejska. Ze względu na mieszany charakter CETA jej pełne wejście w życie wymaga przeprowadzenia odpowiedniej procedury wyrażenia zgody na związanie się nią przez państwa członkowskie Unii Europejskiej, w tym Polskę. Oznacza to, że parlamenty narodowe będą mieć prawo do jej oceny w procesie ratyfikacji.

Mariusz Jabłoński
profesor zwyczajny prawa w Katedrze
Prawa Konstytucyjnego Wydziału Prawa,
Administracji i Ekonomii
Uniwersytetu Wrocławskiego

ZAGADNIENIE WYMOGÓW FORMALNYCH WNIOSKU O UDOSTĘPNIENIE INFORMACJI PUBLICZNEJ

Jedną z cech ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (dalej: udip) jest to, że nie zawiera ona sformalizowanego wzorca wniosku o udostępnienie informacji.

Przez ostatnie kilkanaście lat obowiązywania udip musiały pojawić się oczywiście różnego rodzaju problemy interpretacyjne, w szczególności dotyczące tego, czy wniosek anonimowy (także elektroniczny), który wpływa do zobowiązanego, będzie musiał być przez niego merytorycznie rozpoznany. Przez długi czas ta kwestia była rozstrzygana na korzyść występującego, w tym znaczeniu, że brak podpisu (np. posługiwanie się inicjałami, zamieszczenie imienia lub posłużenie się stwierdzeniem „zaniepokojony obywatel") nie był traktowany jako wada formalna, która uniemożliwiała merytoryczne rozpatrzenie wniosku i w konsekwencji udostępnienie informacji publicznej oraz skarżenie ewentualnej bezczynności zobowiązanego[1].

Praktyka ostatnich kilkunastu miesięcy dostarcza dowodów istotnej zmiany w ocenie zakresu odformalizowania procedury dostępu do informacji publicznej. Po pierwsze, legitymowana do wniesienia skargi konstytucyjnej w zakresie ochrony konstytucyjnego prawa dostępu do informacji publicznej (art. 61 ust. 1 Konstytucji RP) jest wyłącznie osoba fizyczna, posiadająca zdolność procesową, będąca jednocześnie obywatelem polskim (postanowienie TK z 2 grudnia 2015 r., SK 36/14).

Po drugie, uznano, że osoba niepossiadająca pełnej zdolności do czynności prawnych nie dysponuje zdolnością procesową w zakresie dochodzenia realizacji prawa dostępu do informacji publicznej – postanowienie NSA z 21 marca 2017 r., I OSK 2500/16.

Po trzecie wreszcie – co będzie miało najszersze zastosowanie – stwierdzono, że dla złożenia prawidłowego wniosku konieczne jest zamieszczenie w jego treści „co najmniej imienia i nazwiska wnoszącego".

Brak elementu składowego, jakim jest oznaczenie imienia i nazwiska (wniosek anonimowy), skutkuje tym, że w razie gdy na wezwanie zobowiązanego autor wniosku nie dokona samoidentyfikacji, taki wniosek najprawdopodobniej nie zostanie rozpatrzony merytorycznie. W praktyce bowiem zobowiązany będzie wiedział, że anonimowy wnioskodawca jest pozbawiony możliwości skutecznego dochodzenia na drodze sądowej stwierdzenia jego bezczynności. Odmiennie niż miało to miejsce we wcześniejszych wyrokach, sądy uznają, że wniosek, który nie zawiera identyfikacji nadawcy, nie pozwala na ustalenie tożsamości skarżącego z realizującym prawo dostępu do informacji publicznej.

Praktyka taka w zasadzie nie ogranicza realizacji prawa dostępu do informacji publicznej. Jej ukształtowanie ma jednak istotne znaczenie ze względu na konieczność zamieszczenia we wniosku oznaczenia tego, kto z nim występuje. Należy jednocześnie przyjąć, że wystarczy wpisać własne imię i nazwisko (oraz adres w razie wniosku pisemnego), bez konieczności dalszej identyfikacji (także w zakresie korespondencji elektronicznej – kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP). Dane te będą wystarczające do potwierdzenia tożsamości wnioskodawcy ze skarżącym w razie skierowania sprawy do sądu.

1 Warto jednocześnie wskazać, że kwestia oznaczenia wnioskodawcy nie jest zupełnie obojętna. Ma to miejsce w sytuacjach określonych w art. 14 ust. 2, art. 15 ust. 2 udip (powiadomienia), wezwania do wykazania szczególnie istotnego interesu publicznego (art. 3 ust. 1 pkt 1 zd. 2) czy wreszcie wtedy, gdy zachodzi konieczność wydania decyzji o odmowie udostępnienia informacji publicznej. Akty te dla swej skuteczności muszą wiązać się z konkretnym oznaczeniem występującego. Bez tych informacji zobowiązany nie ma bowiem możliwości pełnego zadośćuczynienia swoim obowiązkom wynikającym z udip; zob. szerzej: M. Jabłoński, *Udostępnienie przetworzonej informacji publicznej*, Wrocław 2015, s. 177 i n.

ABI – INSPEKTOREM OCHRONY DANYCH Z MOCY PRAWA?

Arleta Nerka
doktor prawa,
adiunkt w Katedrze
Prawa Pracy ALK

Wprowadzenie IOD jako wykwalifikowanego podmiotu dedykowanego do wykonywania przepisów rodo wywołuje konieczność ustalenia statusu powołanych na gruncie art. 36a uodo ABI po 25 maja 2018 r., czyli po rozpoczęciu stosowania rodo.

Jedną z możliwości, którą należy rozważyć, jest przyjęcie koncepcji, że dotychczasowi ABI pełnią funkcję IOD z mocy prawa. Normatywne zapewnienie ciągłości sprawowanej funkcji bez wątpienia będzie służyło wzmożeniu ochrony interesów podmiotów danych w okresie przejściowym. Poza tym rozwiązanie to można oprzeć na znacznym podobieństwie pozycji ABI i IOD, o czym świadczą zbliżone warunki kwalifikacyjne, usytuowanie organizacyjne w jednostce i charakter niektórych zadań.

W moim przekonaniu wzmocnienie pozycji IOD oraz wprowadzenie nowych obowiązków, zwłaszcza w postaci oceny ryzyka i występowania w stosunkach zewnętrznych administratora danych, wprowadza zupełnie nową jakość w statusie IOD, wymagającą przede wszystkim szerszych umiejętności i kwalifikacji zawodowych. **Stąd administrator danych, licząc się z konsekwencjami ryzyka osobowego, powinien dokonać oceny przygotowania ABI do realizacji funkcji IOD**. Należy zapewnić samodzielność administratorowi danych w zakresie podejmowania decyzji o powołaniu IOD w jednostce oraz o wyborze odpowiedniej osoby do objęcia tego stanowiska, uwzględniającej kryteria wynikające z rodo. Z uwagi na to jako możliwe do przyjęcia przedstawia się kompromisowe rozwiązanie legislacyjne, w myśl którego osoby wykonujące 24 maja 2018 r. funkcję ABI pełnią funkcję IOD do 1 września 2018 r. Po tej dacie z mocy prawa mają zaprzestać pełnienia funkcji IOD, a administrator danych będzie zobowiązany do dokonania notyfikacji swojej decyzji w organie nadzorczym.

Nieunikniona metamorfoza ABI w IOD, do jakiej dojdzie 25 maja 2018 r., wydaje się *prima facie* zabiegiem dość prostym i możliwym do przeprowadzenia nawet w postaci transformacji odbywającej się z mocy prawa.

Należy jednak zwrócić uwagę na potencjalnie negatywne skutki takiego rozwiązania. Gdyby jednak uzyskało ono ostatecznie postać znaną z projektu roboczego nowej uodo, to z uwagi na krótki okres przejściowy (do 1 września) można zakładać, że *de facto* wskazane niżej Konsekwencje nie spowodują trwałego zaburzenia relacji ADO–IOD.

W świetle wymogów stawianych IOD (częściowo nowe zadania i umiejętności oraz co najmniej uzupełniona wiedza – art. 37 ust. 5 rodo) ADO pozbawi się możliwości weryfikacji dotychczasowych ABI w tym zakresie.

Utrwalenie stosunku prawnego łączącego IOD z pracodawcą (art. 38 ust. 3 rodo), wobec częściowo uznaniowego zakresu realizowanych obowiązków i braku szczegółowych kryteriów oceny prawidłowości ich wykonywania, nie pozwoli na swobodną zmianę osób pełniących tę funkcję. Co może być niekorzystne, zwłaszcza w kontekście odpowiedzialności finansowej ADO. W świetle swobody wynikającej z art. 37 ust. 6 rodo utrudni też przekształcenie dotychczasowych relacji prawnych łączących oba te podmioty.

Ponadto konflikt interesów, wskazany w rodo jako granica wykonywania innych zadań przez IOD, może doprowadzić do konieczności ich ograniczenia (wbrew woli ADO) i znalezienia nowych osób zdolnych do realizowania objętych nim obowiązków. Nie bez znaczenia jest też występująca obecnie multiplikacja wykonywania obowiązków ABI przez te same osoby, co może skutkować brakiem realnych możliwości prawidłowego wypełniania zadań IOD.

Krzysztof Wygoda
doktor prawa, pracownik
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

TEMAT NUMERU

Marlena Sakowska-Baryła

OBOWIĄZEK WYZNACZENIA IOD W PODMIOTACH PUBLICZNYCH

Ogólne rozporządzenie o ochronie danych przewiduje obowiązkowe wyznaczenie inspektorów ochrony danych (dalej: IOD) przez organy i podmioty publiczne. **Choć instytucja osoby odpowiedzialnej za nadzór nad systemem ochrony danych osobowych w sektorze publicznym nie jest nowa, to jednak regulacja rodo wymaga większej uwagi**.

Wyznaczenie IOD w sektorze publicznym zostało potraktowane priorytetowo. Ten przypadek obligatoryjnego posiadania IOD został wymieniony na pierwszym miejscu w art. 37 ust. 1 lit. a rodo. Wskazany przepis przewiduje, że administrator i podmiot przetwarzający wyznaczają IOD, zawsze gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

O takim obowiązku nie ma mowy na gruncie obecnie obowiązującej ustawy o ochronie danych osobowych (dalej: uodo), która w art. 36a ust. 1 przewiduje jedynie fakultatywne powołanie ABI, z tym jednak zastrzeżeniem, że w przypadku niepowołania ABI jego zadania określone w uodo wykonuje administrator danych (art. 36b uodo). Dziś tak określony stan dotyczy w równym stopniu zarówno podmiotów publicznych, jak i prywatnych. Bywa, że właśnie w sektorze publicznym wśród podmiotów o podobnym charakterze, wykonujących analogiczne zadania określone w tych samych przepisach prawa znajdziemy takie, które wyznaczyły ABI i dokonały jego rejestracji u GIODO, oraz takie, które ABI nie mają, a przypisane jemu zadania wykonuje sam administrator danych, ewentualnie powierza ich wykonywanie innej osobie (osobom), ale nie tytułując jej ABI, co nie było dotychczas kwestionowane. Tymczasem od 25 maja 2018 r. wraz z rozpoczęciem stosowania rodo każdy podmiot publiczny będzie musiał mieć IOD. U tych, w których wyznaczono ABI, najpewniej dojdzie do sprawnego przekształcenia ABI w IOD. Ułatwi to także ustawodawca, sądząc po art. 59 projektu nowej ustawy o ochronie danych osobowych udostępnionego przez Ministerstwo Cyfryzacji 28 maja 2017 r. (zob. https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych). Jednak te podmioty

w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych – co oznaczono mianem integralności i poufności (zob. art. 5 ust. 1f rodo). Administrator jest odpowiedzialny za przestrzeganie zasad i powinien być w stanie wykazać ich przestrzeganie (art. 5 ust. 2 rodo).

Ustawodawca w rodo nie przewiduje zakazu domniemania czy dorozumiewania zgody. Wyrażenie zgody będzie możliwe przez inne działania osoby, z których jednoznacznie wynika zamiar udzielenia zgody, jednak administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. W art. 8 określono warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego, przyjmując konieczność wyrażania takiej zgody bądź jej zaaprobowania przez osobę sprawującą władzę rodzicielską lub opiekę nad dzieckiem.

W rodo (w stosunku do dyrektywy) rozszerzono zakres danych sensytywnych o dane genetyczne oraz biometryczne, przy czym rodo nie wymaga formy pisemnej zgody na przetwarzanie tego rodzaju danych (zob. art. 9 rodo). W sposób odrębny rodo odnosi się do danych o karalności (dotyczących wyroków skazujących i naruszeń prawa), których przetwarzanie jest dopuszczalne wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem przewidującym odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą, co oznacza ograniczenie dopuszczalności przetwarzania danych o karalności.

Prawa osób, których dane dotyczą

Przepisy rodo wprowadzają rozszerzenie uprawnień osób, których dane są poddawane przetwarzaniu. Zasada przejrzystości przetwarzania ma być realizowana przez szczegółowe informowanie osób, których dane dotyczą, o przetwarzaniu ich danych.

Nowością, jaką wprowadza rodo w ramach obowiązku informacyjnego, jest zobowiązanie do podawania danych kontaktowych inspektora ochrony danych (jeżeli został on powołany), co w zamierzeniu prawodawcy ma ułatwić osobie, której dane dotyczą, realizację jej uprawnień.

DZIAŁANIA PRZYGOTOWUJĄCE DO STOSOWANIA RODO

- Analiza formularzy służących gromadzeniu danych i ocena ich zgodności z wymogami dotyczącymi zgody na przetwarzanie danych oraz dopełnienia obowiązku informacyjnego wynikającego z przepisów rodo.
- Analiza dokumentacji ochrony danych oraz dostosowanie jej do nowych wymogów, zwłaszcza utworzenia rejestru czynności przetwarzania danych, co – jak się wydaje – może być dokonane w oparciu o politykę bezpieczeństwa.
- Przejrzenie umów powierzenia przetwarzania danych pod kątem zgodności z wymogami zawartymi w rodo i dostosowania umów do nowych wymogów.
- Przygotowanie się do spełnienia obowiązków związanych z informowaniem o naruszeniu ochrony danych osobowych. ABI powinien także rozważyć, czy nie zachodzi potrzeba przeprowadzenia oceny skutków dla ochrony danych, o której mowa w art. 35 rodo.
- Przygotowanie się przez osobę mającą pełnić funkcję inspektora ochrony danych osobowych do realizacji nowych zadań. Przepisy krajowe powinny doookreślić, w jaki sposób powinny być realizowane niektóre obowiązki, np. poinformowania organu nadzorczego o danych kontaktowych inspektora.

Przepisy rodo rozszerzają obowiązek informacyjny m.in. o informacje:
- dotyczące okresu przechowywania danych;
- o prawie wniesienia skargi do organu nadzorczego;
- o zautomatyzowanym podejmowaniu decyzji.

Odmiennie zostały uregulowane także wyjątki od obowiązku informacyjnego (zob. art. 13–14 rodo).

Kolejną nowością wprowadzoną na mocy art. 17 rodo jest prawo do bycia zapomnianym. W istocie nie jest to rozwiązanie zupełnie nowe, gdyż bazuje na konstrukcji żądania usunięcia danych, znanej już wcześniej. Prawo do bycia zapomnianym zostało w sposób istotny ograniczone, w stosunku do rozwiązań proponowanych w projektach, przez określenie wyjątków w art. 17 ust. 3 rodo.

W rodo został rozszerzony obowiązek informowania o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania. Zgodnie z art. 35 ust. 3 uodo ten obowiązek dotyczył administratora, który udostępnił zbiór danych, natomiast zgodnie z art. 19 rodo obowiązek informowania obejmuje każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Nowością jest prawo do przenoszenia danych (art. 20 rodo) – osoba, której dane dotyczą, ma prawo:
- otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dotyczące jej dane osobowe, które dostarczyła administratorowi;
- przesłać te dane innemu administratorowi bez przeszkód ze strony administratora, któremu je dostarczono. Uprawnienie to jest jednak ograniczone – przysługuje tylko, gdy przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, bądź przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, a ponadto przetwarzanie odbywa się w sposób zautomatyzowany.

Michał Czerniawski

NOWE PROCEDURY OCHRONY

Unijne przepisy wprowadzają szereg zmian w zakresie uprawnień informacyjnych oraz kontroli i ochrony danych osobowych. Wynika to z dynamiki procesów w przetwarzaniu danych, jakie zachodzą współcześnie. Warto się im przyjrzeć.

W dobie społeczeństwa informacyjnego i powszechnego dostępu do internetu operacje przetwarzania danych osobowych mają coraz bardziej złożony charakter, a uprawnienia podmiotów danych, wynikające z takich aktów prawnych jak dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych czy ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn. DzU z 2016 r., poz. 922) – dalej: uodo – mogą okazać się niewystarczające. Dlatego jednym z założeń unijnej reformy ochrony danych osobowych było zapewnienie podmiotom danych jak najpełniejszej kontroli nad informacjami, które ich dotyczą.

Podstawowym elementem skutecznej kontroli jest posiadanie przez osobę informacji w zakresie tego, co dzieje się z danymi. Dopiero ta wiedza umożliwia podmiotowi danych powzięcie w pełni świadomej decyzji co do konkretnych działań wobec administratora danych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – dalej: rodo – które zacznie być stosowane we wszystkich państwach członkowskich UE od 25 maja 2018 r., wprowadza zmiany w obu tych obszarach:

- uprawnień informacyjnych,
- żądań podjęcia przez administratora danych konkretnych działań.

Uprawnienia informacyjne podmiotu danych

W zakresie uprawnień informacyjnych istotnemu rozszerzeniu uległ zakres informacji, które administrator danych powinien udzielić osobie, której dane dotyczą. W rodo utrzymano znany z dyrektywy 95/46/WE i z uodo podział na sytuacje, w których dane są zbierane bezpośrednio od osoby, której dotyczą, oraz na sytuację, w której dane nie są zbierane bezpośrednio od podmiotu danych. Przepisy art. 13 i 14 rodo zastąpią art. 24 i 25 uodo regulujące zakres informacji, do których udzielenia jest zobowiązany administrator danych. Uzupełniają je postanowienia art. 12 rodo, które doprecyzowują formę, w jakiej informacja powinna być udzielona.

Ustawodawca w art. 13 i 14 rodo dzieli informacje udzielane podmiotowi danych na dwie kategorie informacji:

- takie, których administrator musi udzielić w każdej sytuacji;
- takie, które należy podać, jeżeli są one niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania.

Pojęcie rzetelności i przejrzystości wydaje się dość nieostre. Należy się spodziewać, że ze względów ostrożnościowych, w celu uniknięcia ewentualnych sankcji ze strony organu nadzorczego, administratorzy danych będą udzielać najszerszej możliwej informacji. Jednocześnie w tym zakresie należy spodziewać się wytycznych Europejskiej Rady Ochrony Danych Osobowych – ciała ustanowionego w przepisach rodo, które zastąpi Grupę Roboczą Art. 29.

UPRAWNIENIA PODMIOTU DANYCH INNE NIŻ INFORMACYJNE

- prawo do dostępu;
- prawo do sprostowania danych;
- prawo do usunięcia danych;
- prawo do bycia zapomnianym;
- prawo do ograniczenia przetwarzania;
- prawo do przenoszenia danych;
- prawo do sprzeciwu;
- prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu.

Ustawodawca w art. 12 rodo wprowadza wymóg przejrzystości komunikacji. Ze względu na objętość rozszerzonych klauzul informacyjnych wydaje się, że informacje, o których mowa w art. 13–14 rodo, nie muszą być zawarte, tak jak ma to miejsce najczęściej obecnie, bezpośrednio w klauzuli zgody, ale np. mogą zostać umieszczone na dedykowanej stronie internetowej – na taką możliwość wskazuje wprost motyw 58 rodo.

Dotychczas administrator danych musiał poinformować o:

- swojej nazwie i siedzibie lub miejscu zamieszkania,
- celu zbierania danych,
- przewidywanych odbiorcach,
- prawie dostępu do treści danych oraz ich poprawiania,

a w przypadku zbierania danych nie od osoby, której dotyczą:

- źródle danych,
- możliwości żądania zaprzestania przetwarzania danych oraz wniesienia sprzeciwu.

W przypadku gdy zbieramy dane osobowe z innego źródła niż od osoby, której dane dotyczą, poza wymienionymi informacjami, administrator danych powinien poinformować podmiot danych także o kategoriach danych, których dotyczy przetwarzanie, oraz o pochodzeniu danych, w tym czy pochodzą one ze źródeł publicznie dostępnych. Jednocześnie, w przypadku zbierania danych nie od osoby, której dotyczą, jest przewidziany stosunkowo szeroki wachlarz zwolnień z obowiązku informacyjnego.

Informacji nie trzeba udzielać nie tylko w sytuacji, gdy podmiot danych już je posiada, ale także gdy udzielenie informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Ustawodawca w rodo wprost wskazuje przy tym na przetwarzanie danych osobowych w celach archiwalnych w interesie publicznym, badań naukowych lub historycznych, celów statystycznych, a także sytuacje, gdy spełnienie obowiązku informacyjnego uniemożliwiłoby lub poważnie utrudniło realizację celów przetwarzania. Nie wprowadza przy tym zamkniętego katalogu tego typu sytuacji. Zwolnienie może wynikać także z przepisów prawa krajowego lub unijnego bądź z obowiązku zachowania tajemnicy zawodowej przewidzianego prawem unijnym bądź krajowym.

W przypadku zbierania danych od osoby, której dane dotyczą, obowiązek informacyjny należy spełnić w momencie zbierania tych danych, tak aby podmiot danych mógł się z nimi zapoznać jeszcze przed rozpoczęciem ich przetwarzania. Duża zmiana dla polskich administratorów danych będzie mieć miejsce w odniesieniu do sytuacji, w której dane są zbierane nie od osoby, której dotyczą – art. 25 uodo stanowi bowiem, że informacji należy

NOWE INFORMACJE, KTÓRE ADMINISTRATOR DANYCH JEST ZOBOWIĄZANY PODAĆ PODMIOTOWI DANYCH

- dane kontaktowe administratora (należy zwrócić uwagę, że obecnie obowiązujące przepisy odnoszą się do adresu siedziby lub miejsca zamieszkania, a nie szerszego pojęcia danych kontaktowych. Dane kontaktowe powinny w szczególności obejmować także możliwość kontaktu online – zob. motyw 59 rodo) oraz, gdy ma to zastosowanie, jego przedstawiciela;
- podstawa prawna przetwarzania;
- dane kontaktowe inspektora ochrony danych (jeżeli został powołany);
- prawnie uzasadniony interes realizowany przez administratora lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie tego interesu (art. 6 ust. 1 lit. f rodo);
- zamiar przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, informacja o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony w tym państwie lub organizacji;
- wzmianka o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia, gdy znajduje to zastosowanie (polska wersja językowa rodo jest w zakresie tego obowiązku nieprecyzyjna i błędnie stanowi o „możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych", podczas gdy chodzi o kopie zabezpieczeń lub miejsce ich udostępnienia – należy więc posiłkować się wersją angielską);
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacja o prawie do żądania ograniczenia przetwarzania;
- informacja o prawie do żądania dostępu do danych, ich sprostowania, usunięcia, żądania ograniczenia ich przetwarzania, wniesienia sprzeciwu wobec ich przetwarzania, prawie do przenoszalności danych (dotychczas o możliwości żądania zaprzestania przetwarzania lub sprzeciwu należało informować tylko w przypadku zbierania danych nie od osoby, której one dotyczą);
- informacja o prawie do cofnięcia zgody w dowolnym momencie – bez względu na to, czy na tej podstawie są przetwarzane dane zwykłe czy wrażliwe;
- informacje odnośnie do konsekwencji niepodania danych – gdy podmiot danych jest zobowiązany do ich podania, a także czy podanie danych jest dobrowolne czy jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy;
- informacja o prawie wniesienia skargi do organu nadzorczego;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Anna Kobylańska
Łukasz Ślęzak

BEZPIECZEŃSTWO DANYCH OSOBOWYCH W SEKTORZE FINANSOWYM

Każdy administrator danych osobowych oraz podmioty przetwarzające muszą zapewnić bezpieczeństwo danych osobowych. **Nowe przepisy nakładają na nich dodatkowe obowiązki z tym związane.**

Przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: rodo) została wprowadzona istotna zmiana w podejściu do wymagań zabezpieczania danych osobowych. W miejsce szczegółowych nie zawsze dostosowanych do dostępnych rozwiązań technicznych wymagań odnośnie do organizacyjnych i technicznych środków ochrony danych osobowych w przepisach rodo zostało zawarte wymaganie, by administratorzy i podmioty przetwarzające wdrożyli odpowiednie środki techniczne i organizacyjne, dobrane samodzielnie przez administratora lub podmiot przetwarzający.

Realizacja obowiązku

Sposób spełnienia tego obowiązku dla każdego administratora lub podmiotu przetwarzającego może być inny. Możliwa jest nawet sytuacja, w której w ramach jednego podmiotu konieczne będzie zastosowanie różnych sposobów spełnienia tego wymagania. Należy pamiętać, że każda decyzja o stosowanych środkach bezpieczeństwa danych osobowych powinna być poprzedzona pogłębioną analizą, która pozwoli na wybranie najlepszego rozwiązania.

Zgodnie z art. 32 rodo, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, zapewniające stopień bezpieczeństwa odpowiadający temu ryzyku, m.in. przez:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

Tabela 1: Podsumowanie podobieństw w podejściu do wymagań wynikających z wytycznych KNF oraz przepisów rodo

Perspektywa rodo / wytycznych KNF	Co to oznacza w praktyce?
Sposób osiągnięcia celów, które wynikają z treści przepisów rodo lub wytycznych KNF, może być różny	Podjęte decyzje dotyczące sposobu zapewnienia zgodności z daną rekomendacją lub wymaganiem są kluczowe z perspektywy faktycznego sukcesu wdrożenia właściwych środków ochrony
Sposób osiągnięciach celów zależy od: ▪ specyfiki i profilu ryzyka danego podmiotu ▪ charakterystyki jego środowiska teleinformatycznego ▪ relacji kosztów wprowadzenia danego rozwiązania do wynikających z tego korzyści	Na sukces wdrożenia składają się przede wszystkim dwa elementy: ▪ optymalizacja korzyści z wdrożenia ▪ optymalizacja kosztów wdrożenia
Konieczne jest poprzedzenie każdej decyzji pogłębioną analizą i poparcie jej stosowną argumentacją	Należy pamiętać, że każda decyzja musi być odpowiednio uargumentowana

Fot. 2. Rozpoznanie wzorów i podejmowanie decyzji.

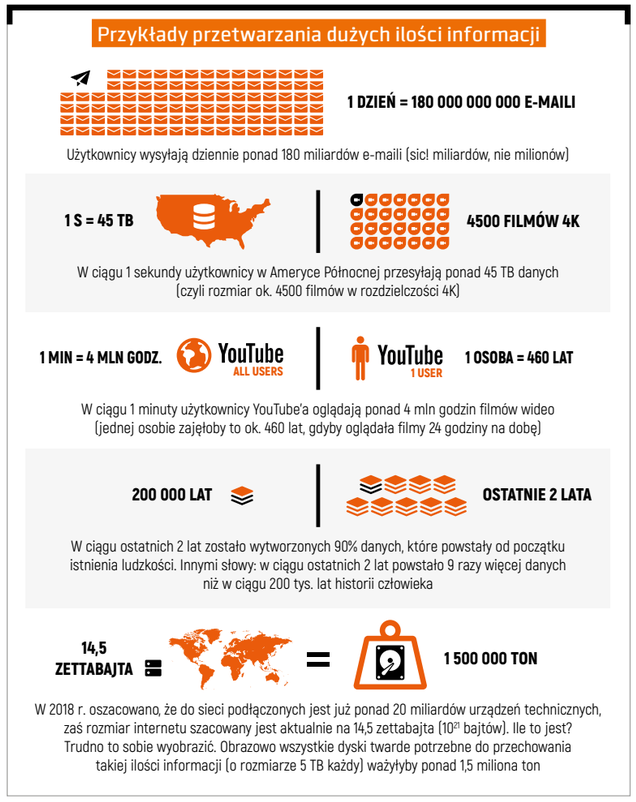
jest bardzo efektywnie realizowane przez rozwiązania takie, jak:

- Hadoop (platforma do rozproszonego składowania wielkich zbiorów danych za pomocą klastrów komputerowych);
- Spark (platforma programistyczna dla obliczeń rozproszonych);
- setki innych narzędzi i rozwiązań wspierających (lista narzędzi ekosystemu big data, https://www.datameer.com/blog/big-data-ecosystem/ [dostęp: 28.01.2019]).

Korzystając z wymienionych technologii, w zależności od potrzeb, możemy przeprowadzić analizy dowolnie dużych zbiorów danych. Stanowi to oczywiście niemałe wyzwanie od strony technicznej (kwestia połączenia wielu rozwiązań w ramach spójnego środowiska pracy), jednakże zarówno sposób organizacji tego środowiska, jak i jego wykonania jest aktualnie dosyć dobrze rozpoznany.

Zgoła odmiennie przedstawia się sytuacja związana z tym, co znajduje się w danych poddawanych analizie. Z uwagi na rozmiar przetwarzanych danych nie ma fizycznej możliwości, aby je zweryfikować i sprawdzić, zanim dokonamy analizy. Może okazać się, że będziemy przetwarzać dane, co do których nie mamy podstaw prawnych, aby takie przetwarzanie realizować. Dostęp do danych mogą uzyskać osoby, które nie powinny mieć tego dostępu (np. dostawca serwisu IT otrzyma informacje o chorobach naszych klientów pozyskane ze źródeł, które w ramach przetwarzania uległy połączeniu po numerze PESEL).

Taka niepewność nie wpływa oczywiście pozytywnie na naszą skłonność do pełniejszego wchodzenia w analizy big data, gdyż powiązane z tym ryzyko może przekraczać zdefiniowany w organizacji poziom „apetytu na ryzyko". Przy ograniczaniu zakresu takich analiz tracimy istotne korzyści biznesowe. Wiedza zawarta w danych nie jest możliwa do uzyskania innymi sposobami. Za jakiś czas taką wiedzę może posiąść nasza konkurencja, co może okazać się ryzykowne dla prowadzonych przez nas działań biznesowych. Na szczęście z pomocą przychodzi nam tzw. uczenie maszynowe oraz algorytmy oparte na sztucznej inteligencji. Zanim jednak przedstawimy pewną propozycję na możliwy zakres wsparcia przez te



Źródło: www.theverge.com

Działania organizacyjne

Powierzenie przetwarzania danych osobowych jest taką usługą, która wymaga specjalnych postanowień w umowie pomiędzy administratorem a podmiotem przetwarzającym. Aby zapewnić wysoki standard ochrony praw i wolności podmiotów danych, warto wdrożyć dodatkowe działania zarówno przed zawarciem umowy powierzenia, jaki i po jej zrealizowaniu.

Tomasz Izydorczyk

Prawodawca unijny w art. 28 ust. 3 rodo wyraźnie zaznacza, że umowa pomiędzy podmiotem przetwarzającym a administratorem musi zawierać: „przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora". Skoro więc prawodawca unijny wymienił oddzielnie przedmiot przetwarzania oraz rodzaj danych osobowych, sformułowanie „przedmiot przetwarzania" należy rozumieć jako konkretne operacje lub zestaw operacji przetwarzania, które zostały wymienione w definicji przetwarzania w art. 4 pkt 2 rodo.

WAŻNE:
Istotą powierzenia przetwarzania danych, jako usługi zleconej przez administratora podmiotowi przetwarzającemu, są operacje na danych i to one właśnie powinny być uzgodnione w pierwszej kolejności pomiędzy administratorem a procesorem.

Natomiast operacje przetwarzania składają się na procesy przetwarzania, które realizowane są w całości lub częściowo przez podmiot przetwarzający.

1

Działania przed zawarciem umowy powierzenia

Prawodawca unijny w przepisach rodo wprowadza nową instytucję gwarancji zapewnienia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie realizowane przez podmioty przetwarzające, spełniało wymogi rodo. Celem tych gwarancji jest ochrona praw osób, których dane dotyczą.

Na czym będą polegać w praktyce wystarczające gwarancje wdrożenia przez procesora odpowiednich środków organizacyjnych i technicznych? Użycie słowa „wystarczające" w stosunku do owych gwarancji daje możliwość różnego podejścia przez różnych administratorów w stosunku do poszczególnych procesów powierzenia przetwarzania. Takie uznaniowe rozumienie gwarancji wpisuje się w podejście oparte na ryzyku, stanowiące jeden z filarów nowej filozofii ochrony dnach osobowych. Dlatego przed powierzeniem przetwarzania danych osobowych podmiotowi zewnętrznemu administrator powinien dokonać oceny ryzyka zgodnie z art. 25 rodo, naruszenia praw i wolności związanego z przyszłym przetwarzaniem zleconym na zewnątrz. W zależności od oszacowanego ryzyka administrator będzie stosował odmienny zestaw środków organizacyjnych i technicznych w stosunku do różnych procesów przetwarzania danych realizowanych przez procesorów.

W zależności od oszacowanego ryzyka administrator będzie stosował odmienny zestaw środków organizacyjnych i technicznych w stosunku do różnych procesów przetwarzania danych.

WDRAŻANIE DZIAŁAŃ PO ZREALIZOWANIU UMOWY

Działania organizacyjne po zrealizowaniu usługi przetwarzania danych osobowych	Kiedy warto wdrażać
1. Weryfikacja, czy dane zwrócone przez procesora są poprawne, np. poprzez porównanie z kopią danych, która została wykonana przed powierzeniem przetwarzania, albo ze specyfikacją danych, która została zatwierdzona przez administratora lub uzgodniona przez obie strony umowy **2.** Przygotowanie przez administratora infrastruktury niezbędnej do przyjęcia danych od procesora – jeśli dane będą zwracane do administratora	■ Przed podpisaniem protokołu zdawczo-odbiorczego, potwierdzającego poprawne zrealizowanie przez procesora usługi i zwrócenie danych do administratora
3. Odebranie oświadczenia od podmiotu przetwarzającego, że dane, które były przetwarzane w imieniu administratora, zostały skutecznie usunięte, także ze wszelkich kopii zapasowych lub archiwalnych	■ Gdy zakres przetwarzanych danych w ramach powierzenia dotyczył danych wyłącznie służbowych pracowników lub innych, które są publicznie dostępne ■ Gdy administrator legitymuje się certyfikatem zgodności, którego zakres pokrywa się z zakresem usługi, jaka była zlecona procesorowi ■ Gdy ryzyko naruszenia praw lub wolności podmiotów danych związanych z powierzeniem przetwarzania było ocenione jako niewielkie czy pomijalne
4. Audyt potwierdzający, że dane zostały skutecznie usunięte, także ze wszelkich kopii zapasowych czy archiwalnych	■ Gdy zakres powierzenia, przedmiot powierzenia był bardzo istotny dla administratora ■ Gdy administrator powierzył przetwarzanie danych, o których mowa w art. 9 lub 10 rodo ■ Gdy znacząca większość procesów przetwarzania danych odbywała się wyłącznie pod kontrolą i za pomocą infrastruktury dostawcy

2

Audyty

Innym działaniem wartym rozważenia przed zawarciem umowy powierzenia przetwarzania będą audyty zgodności potencjalnego dostawcy:
- z wymaganiami rodo,
- z zatwierdzonymi Kodeksami postępowania,
- ze stosownymi normami, np. ISO.

Audyt może być dokonany zarówno przez personel administratora, jak i przez zewnętrznego audytora. Jeśli oferent usługi przetwarzania nie deklaruje zgodności postępowania z branżowym, zatwierdzonym przez organ, kodeksem postępowania, o których mowa w art. 40 rodo, nic nie stoi na przeszkodzie, aby przeprowadzić audyt zgodności z takim kodeksem. Prawodawca unijny w rodo nie wymaga stosowania kodeksów, ale w procesie audytu kodeksy mogą posłużyć jako doskonały punkt odniesienia zarówno dla administratora, jak i procesora. Brak stosowania certyfikatów czy kodeksów postępowania nie oznacza, że potencjalny podmiot przetwarzający nie działa zgodnie z przepisami.

WAŻNE:
Decyzja administratora danych osobowych o wyborze dostawcy, który będzie przetwarzał dane osobowe na jego zlecenie, jest decydowaniem o środkach przetwarzania.

Podmioty przetwarzające

Rozwój cywilizacji spowodowany szybkim postępem technologicznym w wielu dziedzinach życia gospodarczego i społecznego wpłynął na wzrost specjalizacji w sektorach prywatnym i publicznym. Przykładem takich wysoko wyspecjalizowanych jednostek organizacyjnych są przedsiębiorcy przetwarzający dane osobowe na zlecenie administratorów. Typowymi podmiotami przetwarzającymi bywają:
- agencje marketingowe i PR;
- hostingodawcy (usługi centrów przetwarzania danych – „data center");
- dostawcy usług chmurowych (usługi udostępnienia zarówno infrastruktury, jak i usługi wraz z oprogramowaniem w jednym pakiecie);
- biura rachunkowe i kadrowe;
- centra usług wspólnych (tworzone np. przez samorządy terytorialne).

Z drugiej strony podmiotami przetwarzającymi z reguły nie są:
- operatorzy telekomunikacyjni – świadczą usługi na podstawie ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
- Poczta Polska – świadczy usługi pocztowe na podstawie ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe;
- banki – świadczą usługi na podstawie ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

Z różnych przyczyn wielu administratorów korzysta z takich usług (np. hosting, kadry, finanse, archiwum, bhp). Umowa powierzenia będzie regulowała zasady przetwarzania, ale trzeba pamiętać, aby dobrze się przygotować do takiego zlecenia, zaplanować procesy przetwarzania przed wyborem dostawcy, a po zakończeniu usługi być gotowym na przyjęcie danych od procesora bądź na ich usunięcie. ■

Autor jest ABI w ANECOOP Polska sp. z o.o., wykładowcą w Wyższej Szkole Bankowej w Poznaniu oraz konsultantem w kancelarii MARUTA WACHTA sp. j.

WDRAŻANIE DZIAŁAŃ PRZED ZAWARCIEM UMOWY

Działania organizacyjne przed zawarciem umowy powierzenia	Kiedy warto wdrażać
1. Przygotowanie specyfikacji opisującej procesy przetwarzania (w tym operacje), które będą zlecone podmiotowi przetwarzającemu, w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora, ustalenie, czy dane mają być usunięte czy zwrócone mu po zakończeniu usługi	■ Zawsze przed przygotowaniem specyfikacji zamówienia
2. Ocena ryzyka naruszenia praw lub wolności związanych z konkretnym powierzeniem przetwarzania danych osobowych	■ Zawsze przed przygotowaniem specyfikacji zamówienia, ogłoszeniem przetargu, opracowaniem zapytania ofertowego do potencjalnych dostawców
3. Przygotowanie specyfikacji opisującej działania, jakie mają zostać zrealizowane przez procesora po rozwiązaniu umowy **4.** Przygotowanie specyfikacji danych osobowych, m.in. format i struktura danych, dokładny zakres, sposób przechowywania (zapisu), dokładne miejsce przechowywania, zastosowanie konkretnych środków kryptograficznych w stosunku do danych	■ Zawsze przed ogłoszeniem przetargu, opracowaniem zapytania ofertowego do potencjalnych dostawców
5. Sprawdzenie, czy oferent posiada certyfikaty powiązane z ochroną danych (np. ISO 27001, ISO 29134) **6.** Sprawdzenie, czy oferent deklaruje przestrzeganie zatwierdzonych przez organ ochrony danych, kodeksów postępowania	■ Zawsze przed dokonaniem wyboru dostawcy – podmiotu przetwarzającego
7. Weryfikacja zgodności oferenta z przepisami rodo na podstawie oświadczeń oferenta (polegająca na zapoznaniu się z politykami (dokumentami) obowiązującymi u niego **8.** Audyt zgodności oferenta z przepisami o ochronie danych osobowych na podstawie udostępnionych dokumentów, wizyty w miejscach przetwarzania (np. siedzibie) i wywiadami z personelem przyszłego podmiotu przetwarzającego	Zawsze, gdy: ■ zakres powierzenia, przedmiot powierzenia jest bardzo istotny dla administratora ■ administrator zamierza powierzyć przetwarzanie danych, o których mowa w art. 9 lub 10 rodo ■ większość procesów przetwarzania danych będzie odbywała się wyłącznie pod kontrolą i za pomocą infrastruktury dostawcy Niekoniecznie, gdy: ■ np. zakres przetwarzanych danych w ramach powierzenia ma dotyczyć wyłącznie służbowych danych pracowników lub innych, które są lub powinny być publicznie dostępne ■ np. administrator legitymuje się certyfikatem zgodności, którego zakres pokrywa się z zakresem usługi, jaka ma być zlecona procesorowi ■ np. ryzyko naruszenia praw lub wolności związanych z powierzeniem przetwarzania można uznać za niewielkie czy pomijalne
9. Weryfikacja i przygotowanie danych przed przekazaniem ich do przetwarzania procesorowi, może polegać na: a. weryfikacji, czy dane są zgodne z wcześniej opracowaną i zatwierdzoną specyfikacją; b. wykonaniu kopii danych, które będą przekazywane do procesora (w celach porównawczych po zakończeniu świadczenia usług)	■ Po zawarciu umowy o powierzenie przetwarzania danych, jednak przed rozpoczęciem przetwarzania przez dostawcę

Jakub Rzymowski

DOPUSZCZALNOŚĆ PODPOWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zjawisko powierzenia przetwarzania danych osobowych zachodzi od dawna. **Kiedy administrator danych osobowych nie chce lub nie może wykonywać jakiejś czynności osobiście, z wykorzystaniem własnych środków, to zleca jej wykonanie.**

O sobę, której zleca się wykonanie czynności, zwykło się w Polsce nazywać podmiotem (osobą), któremu powierzono przetwarzanie danych osobowych. Z dyrektywy 95/46/WE wynika nazwa: „przetwarzający", która czasem w języku polskim przyjmuje formę: „procesor", co jest niczym innym, jak angielskim słowem *processor*, czyli właśnie przetwarzający.

Zdarza się jednak, że przetwarzający nie chce lub nie może sam wykonywać zleconej mu czynności i dokonuje zlecenia kolejnemu podmiotowi. Tym samym dokonuje podpowierzenia przetwarzania danych osobowych. Podpowierzenie bywa nazywane subpowierzeniem lub dalszym powierzeniem. Powierzenie przetwarzania danych osobowych dotyczy kwestii tak subtelnej, że należy zadać sobie pytanie o to, czy dopuszczalne jest, by podmiot, któremu powierzono przetwarzanie danych osobowych, dokonywał dalszego powierzenia.

Umowa powierzenia przetwarzania danych

Jeżeli administrator powierza przetwarzanie danych osobowych, to musi uczynić to w drodze umowy zawartej na piśmie. Ważne są forma oraz treść umowy.

Forma umowy

Umowa zawarta bez zachowania formy pisemnej też jest ważna, jednak powinno się zachowywać formę pisemną, ponieważ wynika to z art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (DzU z 2016 r., poz. 922) – dalej: uodo.

Dla zachowania formy pisemnej umowy konieczne jest opatrzenie jej własnoręcznym podpisem. W przypadku umowy zawartej w postaci dokumentu elektronicznego konieczne jest podpisanie jej bezpiecznym podpisem elektronicznym weryfikowanym za pomocą kwalifikowanego certyfikatu (uodo) lub podpisem kwalifikowanym (rozporządzenie eIDAS).

Przetwarzanie danych

To każda czynność wykonywana na danych osobowych. Zbieranie, wszelkie czynności wykonywane z przechowywaniem i opracowaniem danych, aż do usunięcia tych danych, oczywiście łącznie z samym usunięciem (art. 7 pkt 2 uodo).

Powierzenie przetwarzania danych

To czynność opisana w art. 31 uodo. Administrator danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi, może powierzyć przetwarzanie danych zwykłych, jak i danych wrażliwych.

- ewidencjonowanie przebiegu zajęć pozalekcyjnych;
- ewidencjowanie przebiegu nauczania;
- ewidencjonowanie procesu egzaminowania;
- ewidencjonowanie świadectw;
- ewidencjonowanie legitymacji;
- zarządzanie i nadzorowanie dokumentacji finansowo-księgowej;
- prowadzenie archiwum.

Kategorie danych, które występują w ramach wskazanych procesów, wyznaczają np.:

- rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów dokumentacji, stanowiące o danych osobowych wpisywanych do księgi uczniów, ewidencji uczniów, dzienników lekcyjnych, czy arkuszy ocen;
- rozporządzenie Ministra Edukacji Narodowej z dnia 26 kwietnia 2018 r. w sprawie świadectw, dyplomów państwowych i innych druków szkolnych, określające dane zawierane w tych dokumentach.

Poza wskazanymi ustawowymi obszarami działalności szkoły każda z jednostek prowadzi własne działania związane z organizacją wydarzeń szkolnych, konkursów, wycieczek. W ich wyniku pojawiają się różne formy dokumentowania tych wydarzeń. W takich przypadkach podstawą przetwarzania danych bywają zgoda i zezwolenie na wykorzystanie wizerunku oraz prawnie uzasadniony interes szkoły. Znajduje to odzwierciedlenie w RCPD przede wszystkim poprzez wyszczególnienie konkretnych procesów przetwarzania danych, takich jak:

- prowadzenie dokumentacji związanej z organizacją wydarzeń szkolnych;
- prowadzenie dokumentacji związanej z organizacją konkursów;
- dokumentowanie wycieczek szkolnych,

oraz przypisanie tym procesom podstawy prawnej zgodnej z zakresem pobieranych na te okoliczności oświadczeń uczestników tych wydarzeń.

ZAKRES RCPD

Zgodnie z art. 30 rodo w rejestrze zamieszcza się:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, gdy ma to zastosowanie, w tym nazwy tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 rodo – dokumentacji odpowiednich zabezpieczeń;
- planowane terminy usunięcia poszczególnych kategorii danych, jeżeli jest to możliwe;
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rodo, jeżeli jest to możliwe.

Prawodawca unijny w przepisach rodo nie definiuje pojęcia „cele przetwarzania", dlatego z praktycznego punktu widzenia zasadne wydaje się rozszerzenie zakresu RCPD o dane porządkujące cele przetwarzania, jakimi mogą być:

- oznaczenia działów lub komórek, w jakich zidentyfikowane zostały konkretne cele przetwarzania;
- nazwy czynności przetwarzania, czyli wykonawczy opis czynności podejmowanych na danych;
- podstawa prawna przetwarzania danych;
- źródło pozyskiwania danych;
- obieg danych wewnątrz organizacji.

Zawartość informacji przedstawianych w rejestrze według wskazanego schematu pokazywać będzie cykl życia danych osobowych w placówce. Jest to ważne, ponieważ z RCPD korzystać będzie administrator nie tylko na potrzeby kontroli, ale także sporządzając obowiązki informacyjne czy realizując prawa osób, których dane dotyczą. W rejestrze wyszczególnione powinny być zatem konkretne czynności przetwarzania danych osobowych. Sposób opisu czynności przetwarzania może zależeć od zakresu zadań przypisanych konkretnym pracownikom i podstawy prawnej przetwarzania danych.

Dodatkowe informacje w RCPD

Opisując w RCPD poszczególne procesy przetwarzania danych osobowych, każdemu z procesów przetwarzania powinniśmy przypisać konkretną podstawę prawną. Uporządkowanie danych poprzez takie zestawienie informacji pozwoli na wykazanie zasad rozliczalności z art. 5 rodo. Ważne jest także określenie w RCPD tego, jaki zakres danych znajduje się w zewnętrznej obsłudze szkoły wynikającej ze zlecenia usług na rzecz podmiotów realizujących outsourcing. Jeżeli dochodzi do powierzenia przetwarzania danych, oprócz wypełnienia obowiązkowej rubryki RCPD o podmiotach przetwarzających rozważenia wymaga potrzeba wpisania sposobu technicznego powierzenia danych, zwłaszcza w sytuacjach tzw. zleceń informatycznych. Wskazanie nazwy wykorzystywanego do obsługi danych oprogramowania uzupełni bowiem część RCPD, która wskazuje na opis technicznych i organizacyjnych środków bezpieczeństwa.

Mając na względzie zasadę aktualizacji danych zawartych w RCPD, użytecznym elementem rejestru jest zaprojektowanie w ramach RCPD kolumny pozwalającej na dokonywanie stosownych wzmianek o dacie i zakresie uzupełnień, zmian i innych modyfikacji RCPD. ■

Autorka jest radcą prawnym, partnerem w Sakowska-Baryła Czaplińska Kancelarii Radców Prawnych Sp.p., doktorantką na Wydziale

Przewodnik po ocenie skutków dla ochrony danych

Ocena skutków dla ochrony danych jest narzędziem, które odpowiednio wbudowane w kulturę organizacyjną zapewni wysoką ochronę danych. Pozwoli na ich bezpieczne przetwarzanie.

Mariola Więckowska

Ocena skutków dla ochrony danych – dalej: OSOD (ang. Privacy Impact Assessment – PIA) – zgodnie z art. 35 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 Kwietnia 2016 r. w sprawie ochrony osób fizycznych w wiązku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: rodo) powinna zostać przeprowadzona w przypadku wysokiego ryzyka naruszenia praw i wolności osoby fizycznej.

Korzyści z OSOD:

- Postępowanie zgodne z ogólnie przyjętymi zasadami etyki.
- Opracowanie strategii ograniczenia ryzyka dla ochrony danych osobowych (dalej: DO).
- Zgodność z rodo.
- Uniknięcie drogich i czasochłonnych zmian, opóźnień i ryzyka niepowodzenia projektu.
- OSOD składa się z kilku etapów.

1

ETAP 1: Wstępna ocena

Ustal, czy w projekcie będzie dochodziło do przetwarzania DO oraz czy projekt będzie stwarzał z dużym prawdopodobieństwem wysokie ryzyko naruszenia praw lub wolności osób – wtedy dalsze etapy OSOD są wymagane.

Rozważ wszystkie aspekty projektu, m.in.:

- dlaczego wprowadzamy zmianę? (np. polepszenie usługi, zwiększenie wydajności, poprawa ochrony prywatności);
- jaka jest podstawa prawna zmiany? (np. wymóg wynikający z przepisów prawa);
- obecny i przewidywany zakres przetwarzanych danych wraz z ich celem i charakterem;
- kategorie przetwarzanych danych: ogólnie dostępne, zwykłe, szczególne;
- skutki łączenia informacji z innymi danymi;
- nośniki danych, np. papier, dane elektroniczne i ich rodzaj;
- użycie nowych technologii;
- ocenę poziomu ryzyka i związaną z tym decyzję o przeprowadzeniu pełnego OSOD.

Łączone informacje mogą potencjalnie zwiększyć ryzyko zidentyfikowania osoby przez wnioskowanie, nawet jeśli sama informacja nie jest uważana za dane osobowe.

Udokumentuj:

A. Nazwa projektu
B. Właściciel biznesowy lub organizacja
C. Osoba kontaktowa
D. Kluczowe daty
E. Zwięzły opis projektu z uwzględnieniem celu biznesowego
F. Obecny i przewidywany zakres przetwarzanych danych
G. Charakter danych – w OSOD rodzaj przetwarzanych danych to, np. dane zwykłe, dane szczególne (dane genetyczne, biometryczne lub dotyczące zdrowia)
H. Kontekst przetwarzanych danych – okoliczności oraz otoczenie, w którym są przetwarzane DO (np. kontekst publiczny lub prywatny)
I. Ocena poziomu ryzyka – decyzja o przeprowadzeniu pełnego OSOD

PAMIĘTAJ:

- Udokumentuj ten etap OSOD, aby zgodnie z zasadą rozliczalności móc wykazać przed organem nadzorczym wypełnienie obowiązku z rodo.

2

ETAP 2: Ocena skutków dla ochrony danych

Rozpocznij od szczegółowej analizy projektu w celu identyfikacji potencjalnego wpływu zmiany na prywatność. Rozważ m.in.:

- główne cechy projektu, które mogą stwarzać zagrożenie prywatności;
- działania i procesy biznesowe oraz przepływy informacji, na które wpłynie zmiana.

UDOKUMENTUJ:

A. Opis planowanych operacji przetwarzania i celów przetwarzania, w tym:
- realizowanych przez administratora interesów prawnych;
- jak, kto i z jakimi uprawnieniami będzie je przetwarzał;
- jaka technologia będzie stosowana.

B. W jaki sposób i kiedy DO będą mogły być przetwarzane poza jednostką organizacyjną, szczególnie w państwach trzecich.
C. Przepływ DO przez istniejące i przyszłe systemy lub procesy biznesowe.

Elementy raportu OSOD

A. Strona tytułowa z nazwą projektu, datą przeprowadzenia i osobą odpowiedzialną za OSOD
B. Streszczenie
C. Wstępna ocena
D. Analiza projektu
E. Identyfikacja zagrożeń i ich potencjalnych skutków dla prywatności
F. Ocena ryzyka prywatności i rekomendowane środki zaradcze
G. Decyzje i zgody na wprowadzenie środków zaradczych lub akceptację ryzyka
H. Dalsze działania, w tym konsultacje z organem nadzorczym w przypadku wysokiego ryzyka przed rozpoczęciem przetwarzania
I. Przypadki, w których należy dokonać przeglądu niniejszej oceny
J. Załączniki

Zacznijmy od definicji...

Przetwarzanie według rodo

to zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnienie poprzez przesłanie, rozpowszechnienie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

3

ETAP 3: Ocena ryzyka prywatności i rekomendowane środki zaradcze

Podstawą oceny ryzyka prywatności jest zrozumienie prawdopodobieństwa naruszenia praw i wolności osób, których dane dotyczą, i wiążących się z tym potencjalnych skutków. Ocena jest niezbędna do identyfikacji środków zaradczych i działań oraz do wydania rekomendacji, co do sposobu realizacji projektu, które zminimalizują ryzyko prywatności i wzmocnią potencjalne korzyści z lepszej ochrony danych. Pozwala wybrać te środki zaradcze, które są najbardziej korzystne dla podmiotów danych, projektu i administratora danych.

Do tej pory oceniane było ryzyko wiążące się z przetwarzaniem danych, rodzące skutki finansowe, prawne i utraty reputacji w wyniku naruszenia prywatności oraz konsekwencje nieprzestrzegania przepisów. Przepisy rodo wprowadzają ryzyko naruszenia praw lub wolności osób, w tym braku wypełniania praw osób, możliwości kradzieży tożsamości, naruszenia dobrego imienia, dyskryminacji lub negatywnych skutków finansowych.

UDOKUMENTUJ:

Dla każdego ryzyka:
A. Źródło ryzyka (z powodu...).
B. Ryzyko (istnieje ryzyko, że...).
C. Potencjalne skutki (w wyniku czego...).
D. Istniejące środki bezpieczeństwa.
E. Poziom prawdopodobieństwa i wpływ skutków przy obecnych środkach bezpieczeństwa.

Dobór środków zaradczych

Dla każdego potencjalnego ryzyka prywatności określ możliwe środki zaradcze i działania, które je wyeliminują lub zmniejszą. Typowe rozwiązania obejmują zwykle:

- rezygnację z przetwarzania części DO;
- ograniczenie czasu przechowywania danych i zaplanowanie ich bezpiecznej likwidacji;
- wdrożenie odpowiednich technologii, procesowych i fizycznych środków zabezpieczeń;
- zastosowanie pseudonimizacji lub anonimizacji danych;
- przygotowanie instrukcji o sposobie używania nowego systemu i odpowiednie przeszkolenie pracowników;
- zapewnienie transparentności informacji podmiotom danych (jakie dane i w jaki sposób są przetwarzane);
- wybór dostawców oferujących większy poziom bezpieczeństwa.

PAMIĘTAJ:

- Minimalizacja danych to środek zmniejszający ryzyko przetwarzania danych.

Dobierz adekwatne środki zaradcze opierając się na ocenie skuteczności poszczególnych rozwiązań. Wybierz te, które są najbardziej korzystne dla podmiotów danych, projektu i administratora danych.

UDOKUMENTUJ:

A. Rekomendowane środki mitygacji ryzyka.
B. Poziom prawdopodobieństwa i wpływ skutków po zastosowaniu rekomendowanych środków.

4

ETAP 4: Przygotowanie raportu końcowego

Zadaniem OSOD jest wsparcie celów projektu i dostarczenie kluczowym interesariuszom propozycji strategii ograniczenia ryzyka prywatności w celu podjęcia świadomych decyzji. Ocena skutków dla ochrony danych udokumentuje należytą staranność względem ochrony DO i wykaże stosowanie ochrony danych w fazie projektowania oraz domyślną ochronę danych.

PAMIĘTAJ:

- Dla każdego rekomendowanego środka zaradczego ograniczającego ryzyko określ konkretne działania, osobę odpowiedzialną i termin realizacji. Wszelkie decyzje dotyczące prywatności i wybranych działań powinny być odpowiednio udokumentowane i zaakceptowane.

Zidentyfikowane działania są konieczne do uzyskania zgodności z rodo i tworzą strategię ograniczenia ryzyka prywatności.

Identyfikacja zagrożeń i ich potencjalnych skutków dla prywatności

Korzystając z informacji zebranych w analizie projektu, zidentyfikuj potencjalne zagrożenia i ich wpływ na ochronę prywatności. Przykładowe zagrożenia to:

- brak podstawy prawnej do zbierania, wykorzystywania lub ujawniania DO;
- przetwarzanie nieprecyzyjnej, niewystarczającej lub nieaktualnej informacji;
- nieuzasadnione użycie lub ujawnienie DO, np. gdy spseudonimizowane lub anonimowe dane są wystarczające, aby osiągnąć cel;
- zbyt szeroki zakres przetwarzanych danych;
- przetwarzanie danych niezgodnie z pierwotnym celem;
- przetwarzanie danych po wygaśnięciu celu ich przetwarzania;
- ujawnienie DO nieuprawnionym podmiotom;
- brak zachowania odpowiedniego poziomu bezpieczeństwa;
- brak możliwości wypełnienia praw podmiotów danych;

UDOKUMENTUJ:

A. Zidentyfikowane zagrożenia prywatności i skutki, odnosząc się do wszystkich aspektów projektu, w tym powiązań procesów biznesowych i użytych technologii.

B. Istniejące środki ochrony prywatności dla planowanych działań, które mogą mieć zastosowanie do poszczególnych zagrożeń.

WSKAZÓWKI

- Na każdym etapie OSOD korzystaj z wiedzy ekspertów IT, zarządzania, ryzyka, bezpieczeństwa, prawa i prywatności oraz właścicieli biznesowych.
- Dla podobnych operacji przetwarzania danych wiążących się z podobnym ryzykiem przeprowadź pojedynczą ocenę.
- Pamiętaj, kto jest odbiorcą OSOD. To nie ma być ocena technicznych aspektów systemu, ale ocena skutków zmiany wobec ochrony DO. Dołóż starań, aby informacje były przedstawione w sposób prosty i zrozumiały dla odbiorcy, który nie posiada wiedzy na temat technologii, prawa lub tego systemu.
- Unikaj żargonów i skrótów, gdy nie są powszechnie zrozumiałe, chyba że je wyjaśnisz.
- Informacje powinny być wyczerpujące, ale zwięzłe i jedynie niezbędne do zrozumienia OSOD.

5

ETAP 5: Monitoring wdrożenia

Śledź postępy działań związanych z ochroną prywatności, aby upewnić się, że są odpowiednio zakończone. Oceniaj wszelkie zmiany w realizacji projektu, procesów biznesowych, przepływu informacji, ról i zadań, aby upewnić się, że nie powstaje nowe ryzyko prywatności. ■

Autorka pracuje w Grupie Allegro jako ABI; pomaga wykorzystywać nowe technologie informatyczne w zgodzie z obowiązującymi zasadami ochrony i bezpieczeństwa danych osobowych.

06. School agendas and schedules for students and parents

This is my one of the largest and most technically advanced publishing projects! The project is also a perfect example of what effects automation brings. I used the theory of regular expressions (regex) with the corresponding Adobe graphical tools and open-source: Perl, Curl, grep, AWK and sed.
To ensure proper organization of work on such a large project, I prepared a dedicated publication typesetting subsystem, which ultimately generated almost 58 unique, 100-page editions for printing based on only three production files of the Adobe InDesign publication typesetting program.

Scope of work:
– design
– layout
– typography
– creation of a system for text processing and automation of preparation for printing of final editions
– desktop publishing
– pre-press

↑ Click to move to Table of Contents

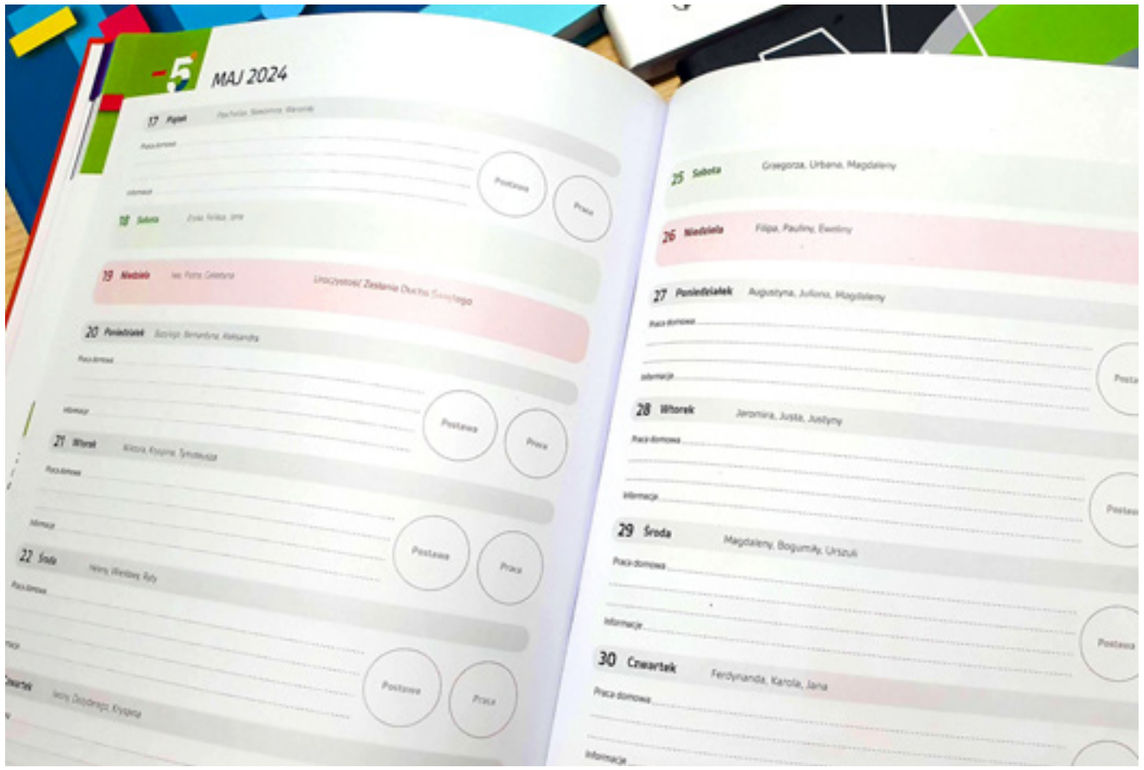

OPTYMISTA
4–latki


5
SZCZEROŚĆ
SPRÓBUJ SWOICH SIŁ
MÓJ BOHATER
Zofia Kossak-Szczucka
SZCZEROŚĆ
Mówienie prawdy, wyrażanie tego, co się myśli
MAJ
6–10
22
Aby żyć w zgodzie z innymi, człowiek musi najpierw pogodzić się z samym sobą
BIBLIOTECZKA MĄDROŚCI
TUTORING
z przewodnikiem łatwiej
MY LUBIMY POEZJĘ
POLSKA


MĘSTWO
DECYDUJĄ SZCZEGÓŁY
AKTUALNE OD 2010 R.
Forti et fideli nihil difficile
Dla dzielnego i wiernego nic nie jest trudne
MÓJ KAWAŁEK PODŁOGI
NARODZIŁ ZAMKNIĘTA W SŁOWA
Komizelka
PŁYN POEZJI
Pieśń poranna
PANTEON PATRONÓW
Filippo Brunelleschi
SCIENCE
Florencja


Styczeń
Od najmłodszych lat:
J. KOLĘDA!
TUTORINGOWY GPS
Słowa, które zmieniają:
Spójrz w oczy dziecka – zobaczysz Boga
Phil Bosmans
Z powagą nam do twarzy
Camille Saint-Saëns (1835–1921)
Śpiewam z tatą, śpiewam z mamą
Widzieć niewidzialne
Temat: Chrzest Pana Jezusa
Dzień Babci


Od najmłodszych lat:
MĄTCZYNIA MIŁOŚĆ
TUTORINGOWY GPS
Słowa, które zmieniają:
Tyle wart jest nasz rok, ile zdołaliśmy okazać ludziom serca, bliskości, współczucia, dobroci i pociechy
kard. Stefan Wyszyński
Ojcowie na Start
Święto Rodziny
Piotr Czajkowski (1840–1893)
Śpiewam z tatą, śpiewam z mamą
Żyrafa fa fa
Agnieszka Galica
Widzieć niewidzialne
Temat: Życie Maryi
Wierszem malowane
Jan Brzechwa
„Zoo"
#Powiedzmy to razem


MAJ 2024
25 Sobota Grzegorza, Urbana, Magdaleny
26 Niedziela Filipa, Pauliny, Ewelin
27 Poniedziałek Augustyna, Juliana, Magdaleny
28 Wtorek Jeronima, Justa, Justyny
29 Środa Magdaleny, Bogumiły, Urszuli
30 Czwartek Ferdynanda, Karola, Jana

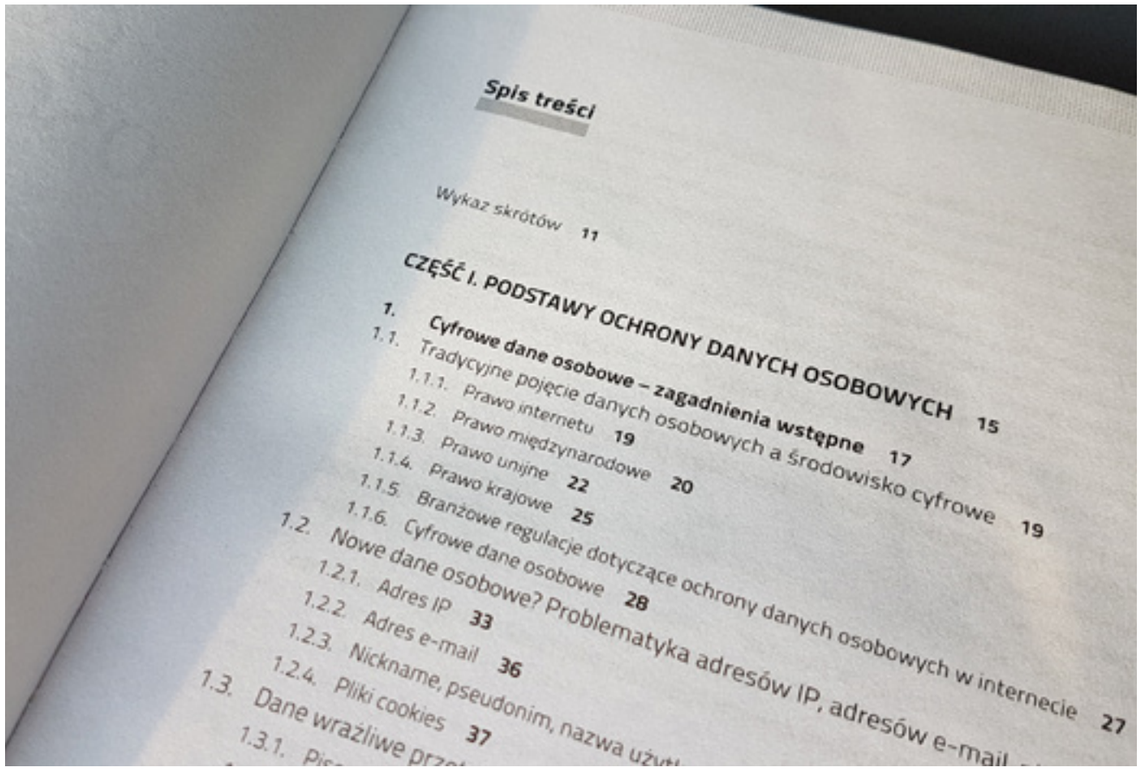

DECYDUJĘ SAM
AKTUALNIE OD ZAJĘĆ
Non scholae, sed vitae discimus
Uczymy się nie dla szkoły, lecz dla życia
MÓJ KAWAŁEK PODŁOGI
ALERT!
10
Wieczornica Patriotyczna
11
Święto Niepodległości
20
MĄDROŚĆ ZAMKNIĘTA W SŁOWA
Legendy polskie
PŁYŃ POEZJO Z POTOKIEM
Ulewa
SCIENCE
PANTEON PATRONÓW
Zofia Kossak
Polska
Bielsko-Biała
22-23
27
28
Wykład dla rodziców


POSŁUSZEŃSTWO
POSŁUSZEŃSTWO, czyli CO?
#JEDNYM ZDANIEM
POSŁUSZEŃSTWO
Wypełnianie poleceń, przestrzeganie zasad
BIBLIOTECZKA MĄDROŚCI
Najmilsi
PODEJMIJ WYZWANIE:
MY LUBIMY POEZJ
PISANKI
KWIECIEŃ
Wyjście do muzeum
Międzyszkolny konkurs recytatorski Wrocławski Krasnal", etap klasowy
Międzyszkolny konkurs recytatorski Wrocławski Krasnal", finał

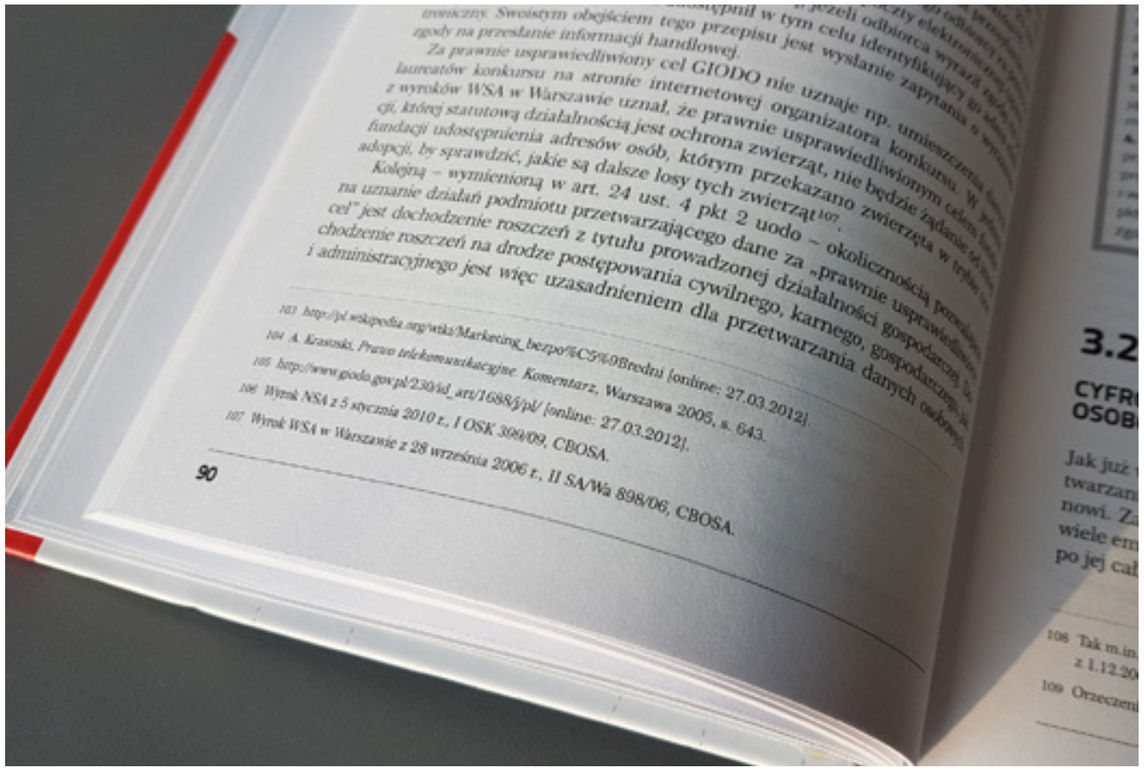
07. Book #1 – design and typography

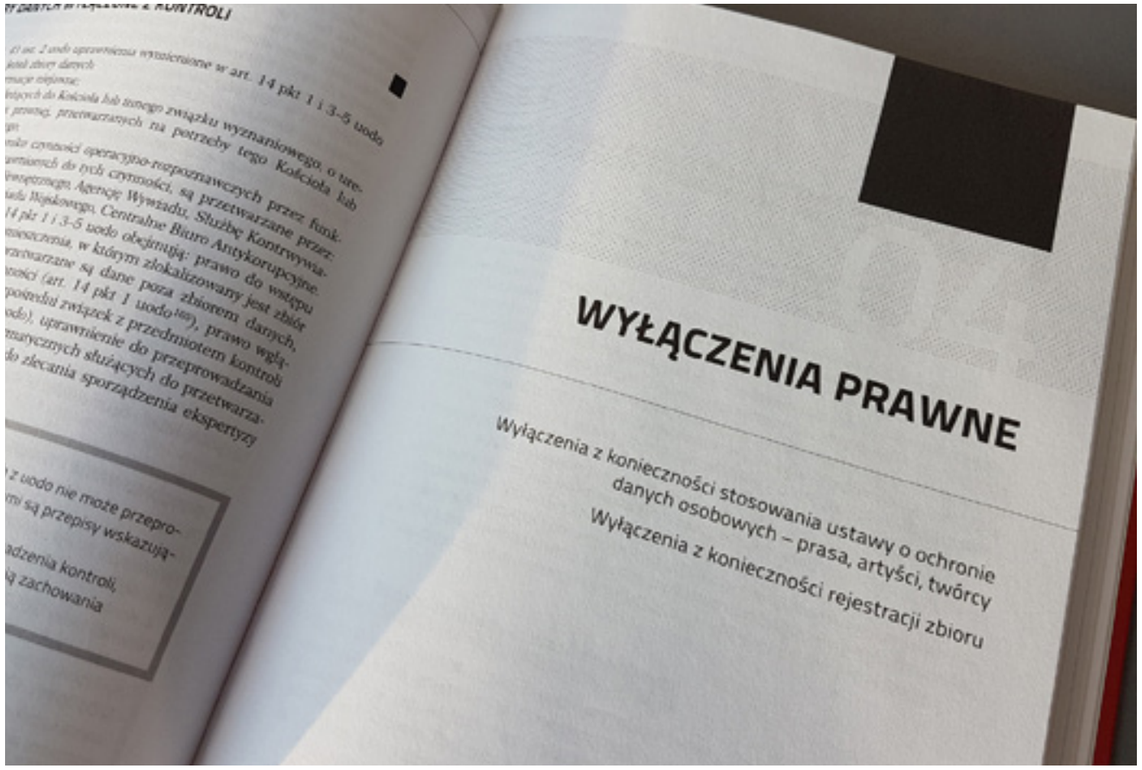
Scope of work:
– design
– layout
– typography
– desktop publishing
– pre-press

↑ Click to move to Table of Contents



Spis treści



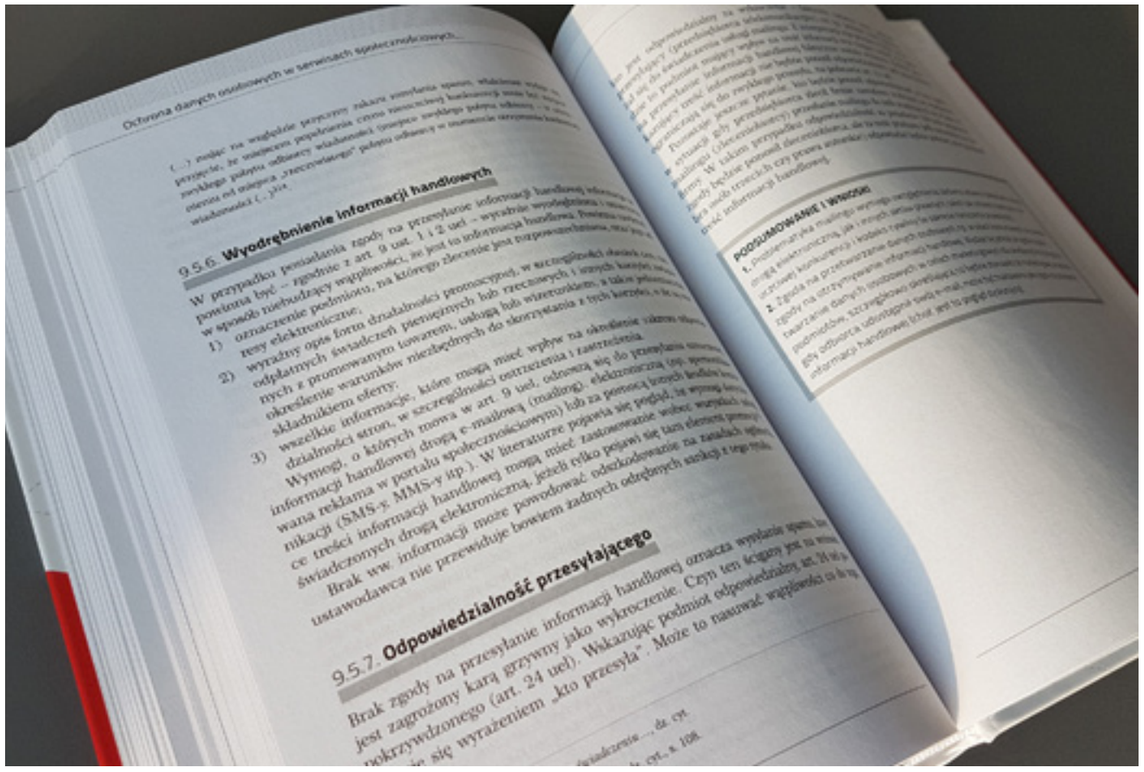


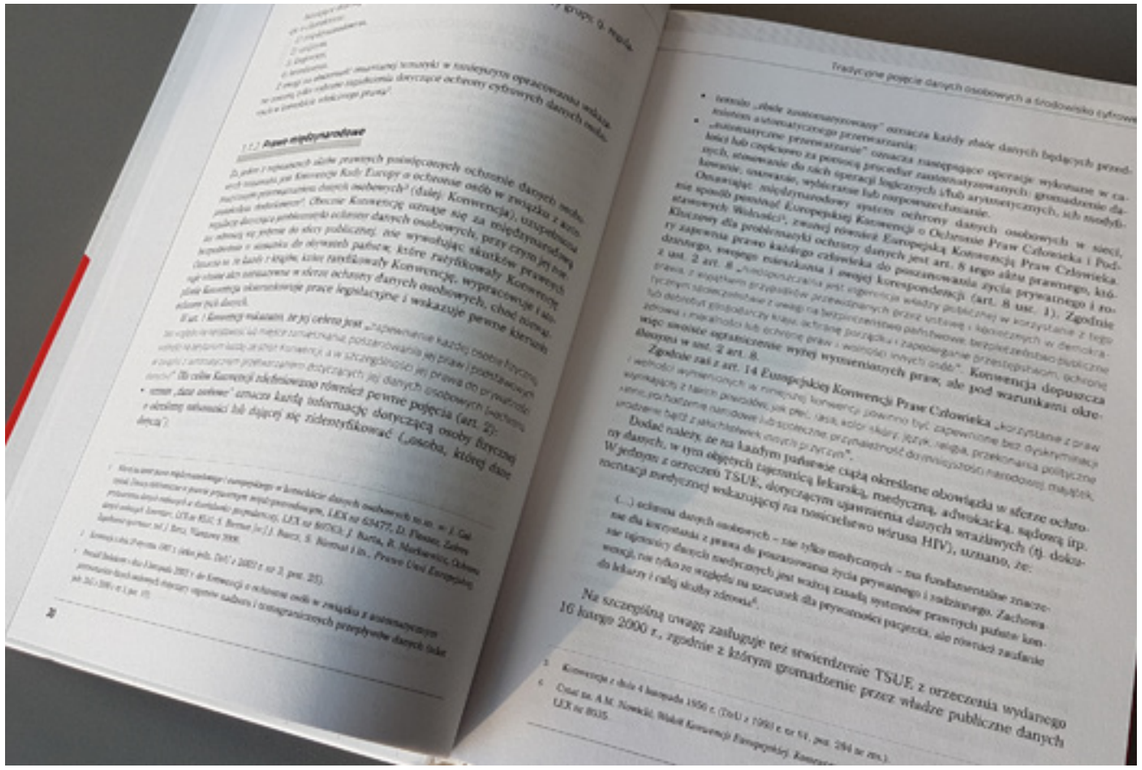
WYŁĄCZENIA PRAWNE

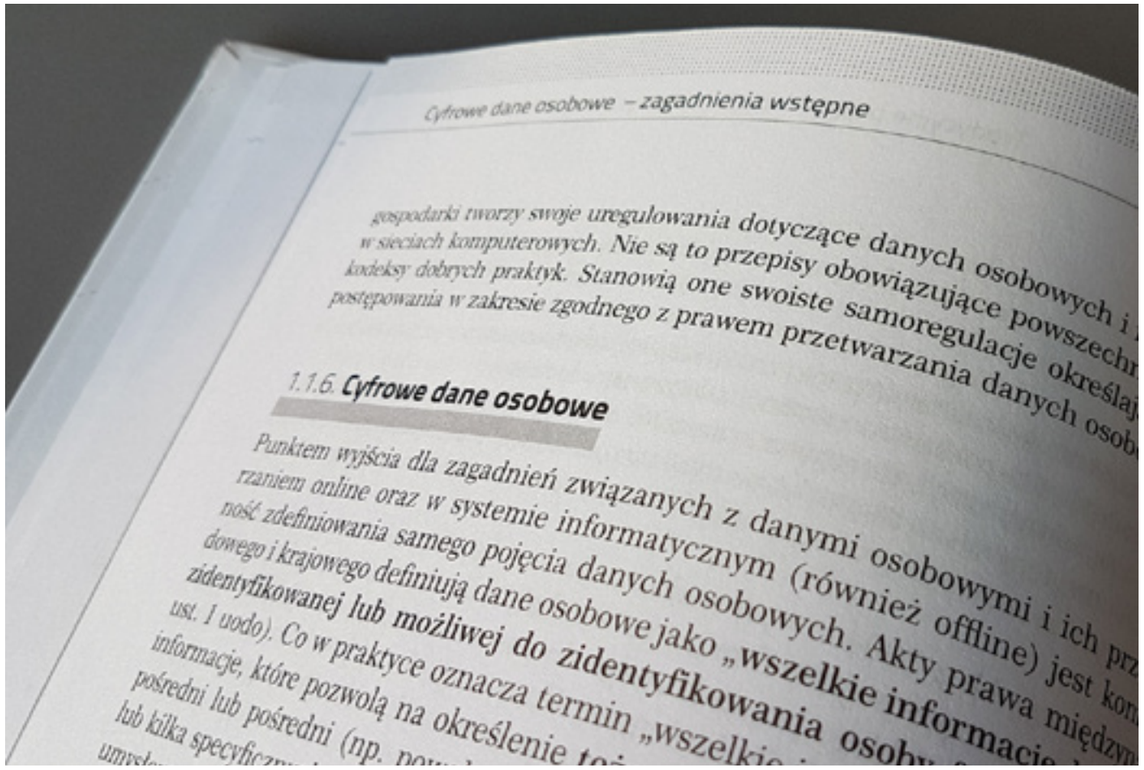
Wyłączenia z konieczności stosowania ustawy o ochronie danych osobowych – prasa, artyści, twórcy

Wyłączenia z konieczności rejestracji zbioru


CZĘŚĆ III
DANE OSOBOWE
W ADMINISTRACJI PUBLICZNEJ


Ochrona danych osobowych w serwisach społecznościowych
9.5.6. Wyodrębnienie informacji handlowych
9.5.7. Odpowiedzialność przesyłającego
PODSUMOWANIE I WNIOSKI

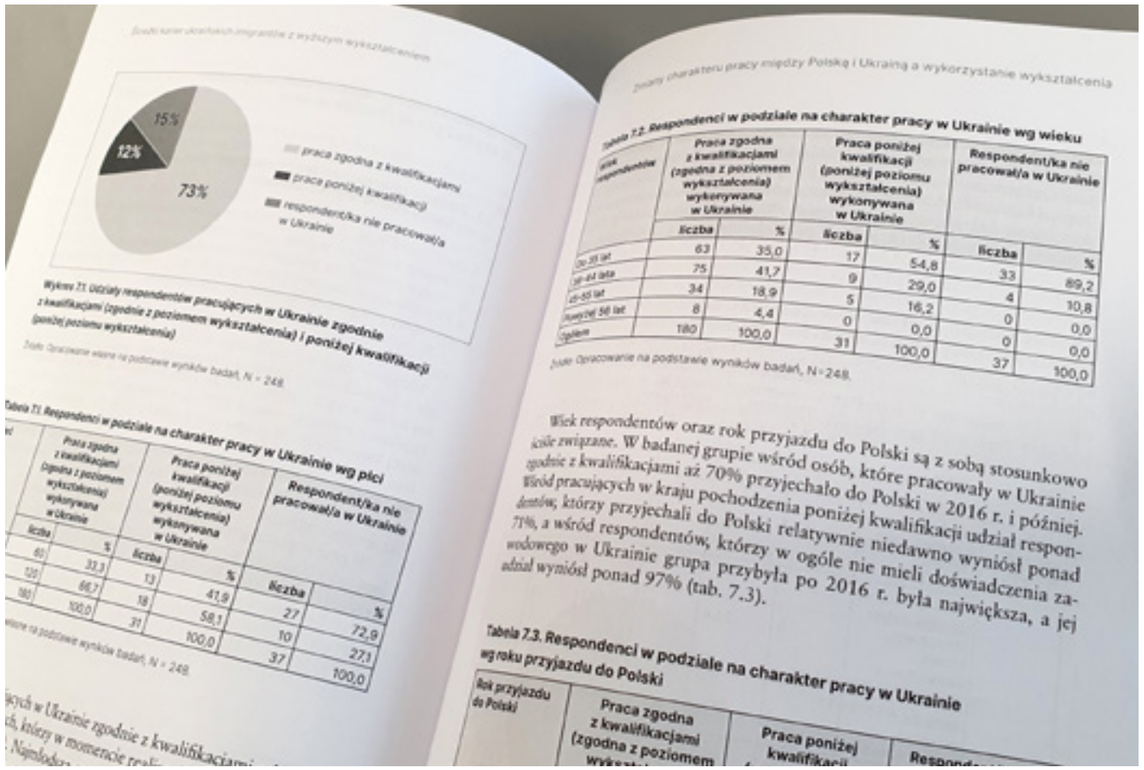

Tradycyjne pojęcie danych osobowych a środowisko cyfrowe


Cyfrowe dane osobowe – zagadnienia wstępne
1.1.6. Cyfrowe dane osobowe

08. Book #2 – design and typography

Scope of work:
– design
– layout
– typography
– design of infographics, diagrams and charts
– desktop publishing
– pre-press

↑ Click to move to Table of Contents



Wykres 7.1. Udziały respondentów pracujących w Ukrainie zgodnie z kwalifikacjami (zgodnie z poziomem wykształcenia) i poniżej kwalifikacji (poniżej poziomu wykształcenia)

Źródło: Opracowanie własne na podstawie wyników badań, N = 248.

Tabela 7.1. Respondenci w podziale na charakter pracy w Ukrainie wg płci

	Praca zgodna z kwalifikacjami (zgodna z poziomem wykształcenia) wykonywana w Ukrainie		Praca poniżej kwalifikacji (poniżej poziomu wykształcenia) wykonywana w Ukrainie		Respondent/ka nie pracował/a w Ukrainie	
	liczba	%	liczba	%	liczba	%
	60	33,3	13	41,9	27	72,9
	120	66,7	18	58,1	10	27,1
	180	100,0	31	100,0	37	100,0

Tabela 7.2. Respondenci w podziale na charakter pracy w Ukrainie wg wieku

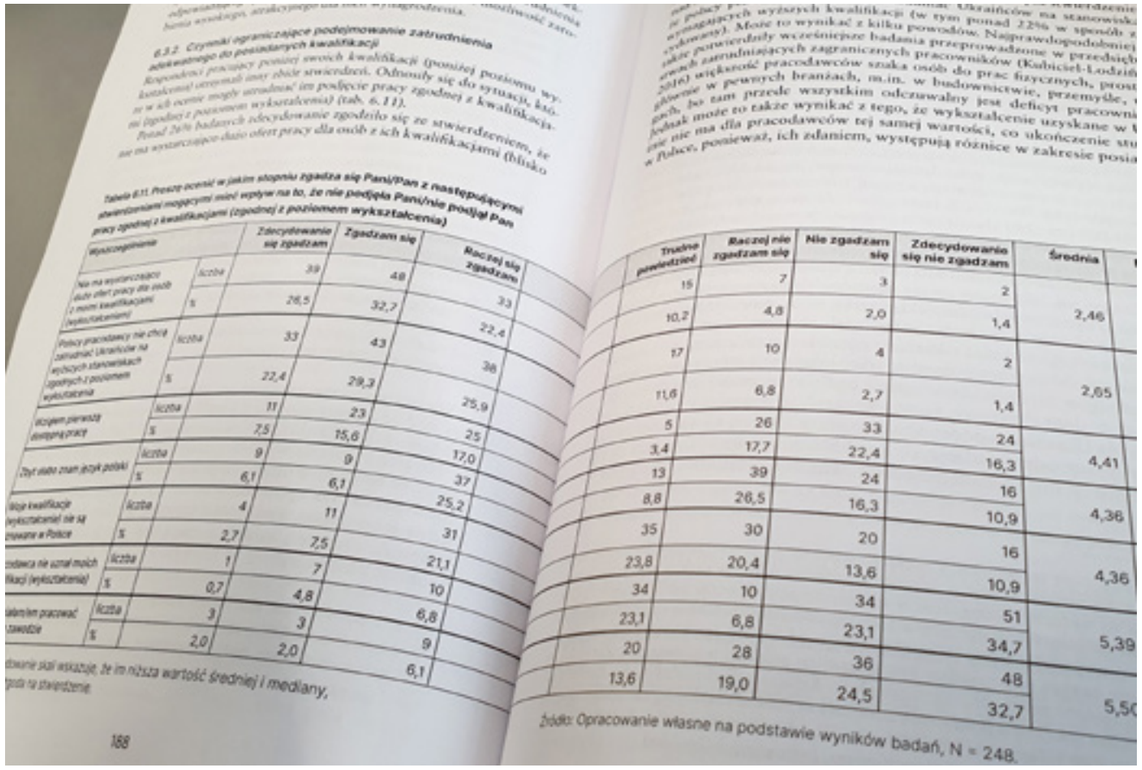
Wiek respondentów	Praca zgodna z kwalifikacjami (zgodna z poziomem wykształcenia) wykonywana w Ukrainie		Praca poniżej kwalifikacji (poniżej poziomu wykształcenia) wykonywana w Ukrainie		Respondent/ka nie pracował/a w Ukrainie	
	liczba	%	liczba	%	liczba	%
Do 35 lat	63	35,0	17	54,8	33	89,2
36–44 lata	75	41,7	9	29,0	4	10,8
45–55 lat	34	18,9	5	16,2	0	0,0
Powyżej 56 lat	8	4,4	0	0,0	0	0,0
Ogółem	180	100,0	31	100,0	37	100,0

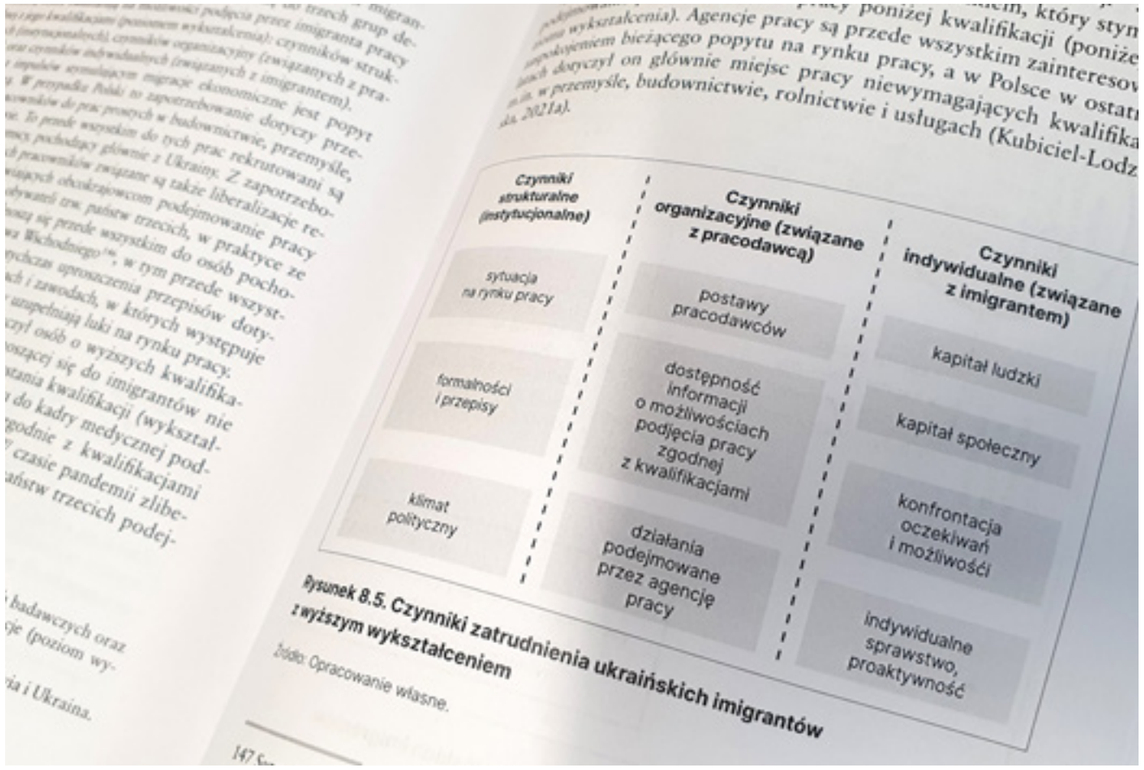
Źródło: Opracowanie na podstawie wyników badań, N = 248.

Wiek respondentów oraz rok przyjazdu do Polski są z sobą stosunkowo ściśle związane. W badanej grupie wśród osób, które pracowały w Ukrainie zgodnie z kwalifikacjami aż 70% przyjechało do Polski w 2016 r. i później. Wśród pracujących w kraju pochodzenia poniżej kwalifikacji udział respondentów, którzy przyjechali do Polski relatywnie niedawno wyniósł ponad 71%, a wśród respondentów, którzy w ogóle nie mieli doświadczenia zawodowego w Ukrainie grupa przybyła po 2016 r. była największa, a jej udział wyniósł ponad 97% (tab. 7.3).

Tabela 7.3. Respondenci w podziale na charakter pracy w Ukrainie wg roku przyjazdu do Polski

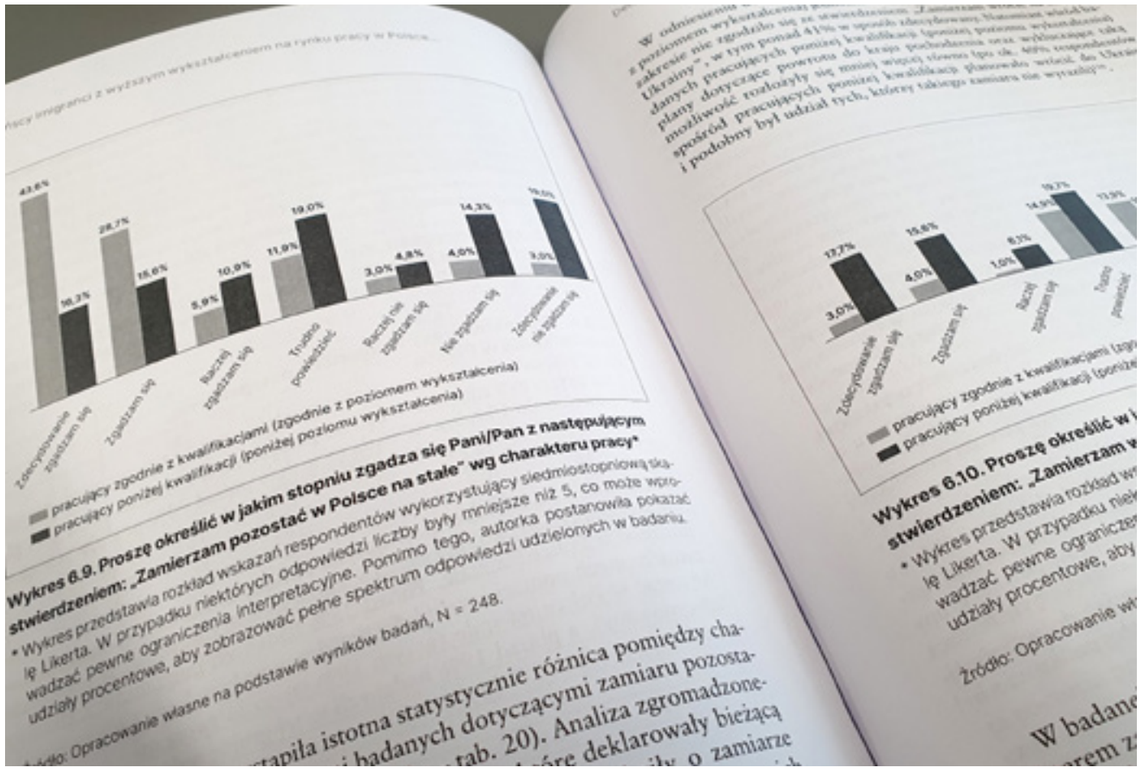
Rok przyjazdu do Polski	Praca zgodna z kwalifikacjami (zgodna z poziomem	Praca poniżej kwalifikacji	Respon





Rysunek 8.5. Czynniki zatrudnienia ukraińskich imigrantów z wyższym wykształceniem

Źródło: Opracowanie własne.



Wykres 6.9. Proszę określić w jakim stopniu zgadza się Pani/Pan z następującym stwierdzeniem: „Zamierzam pozostać w Polsce na stałe" wg charakteru pracy*

* Wykres przedstawia rozkład wskazań respondentów wykorzystujący siedmiostopniową skalę Likerta. W przypadku niektórych odpowiedzi liczby były mniejsze niż 5, co może wpływać pewne ograniczenia interpretacyjne. Pomimo tego, autorka postanowiła pokazać udziały procentowe, aby zobrazować pełne spektrum odpowiedzi udzielonych w badaniu.

Źródło: Opracowanie własne na podstawie wyników badań, N = 248.

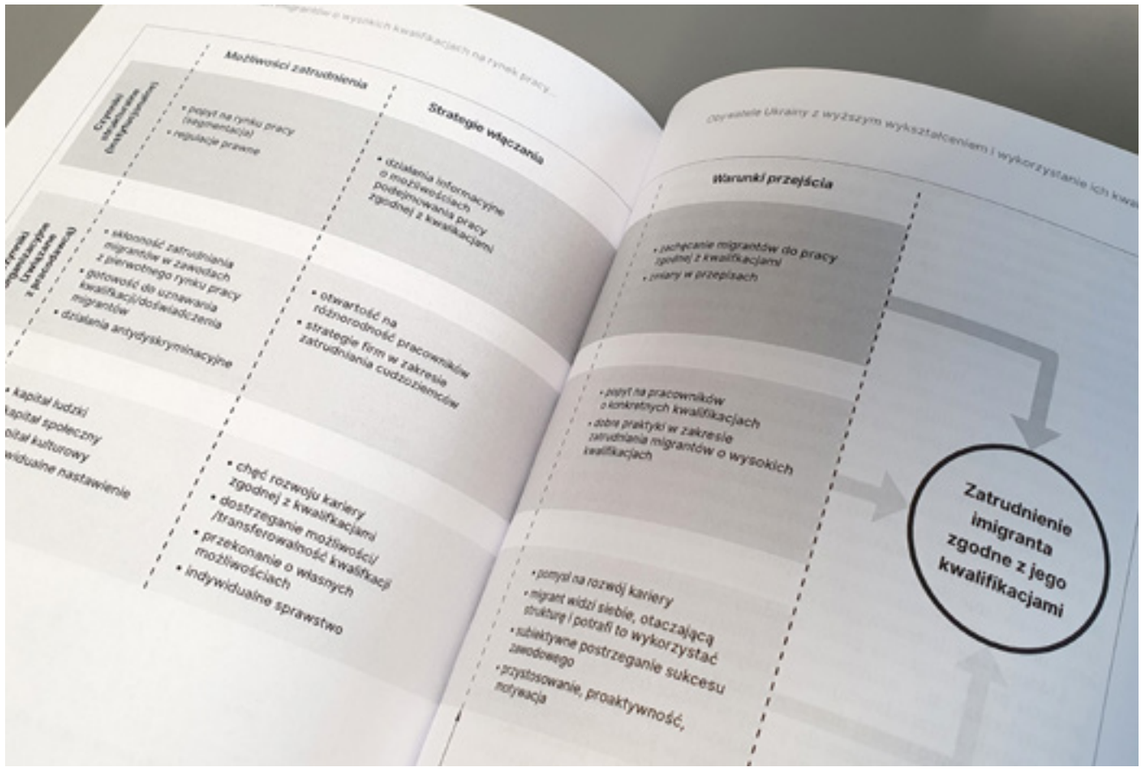
stąpiła istotna statystycznie różnica pomiędzy cha- badanych dotyczącymi zamiaru pozosta- tab. 20). Analiza zgromadzone- które deklarowały bieżącą ły, o zamierze

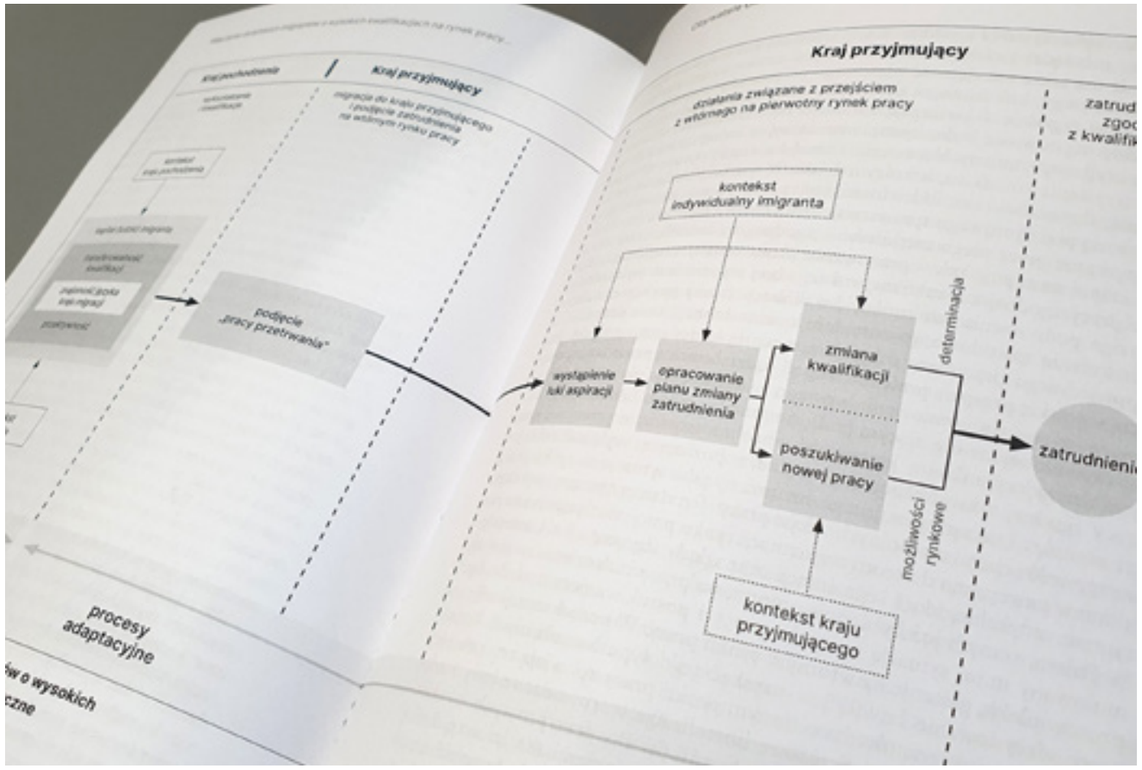
Wykres 6.10. Proszę określić w
stwierdzeniem: „Zamierzam w

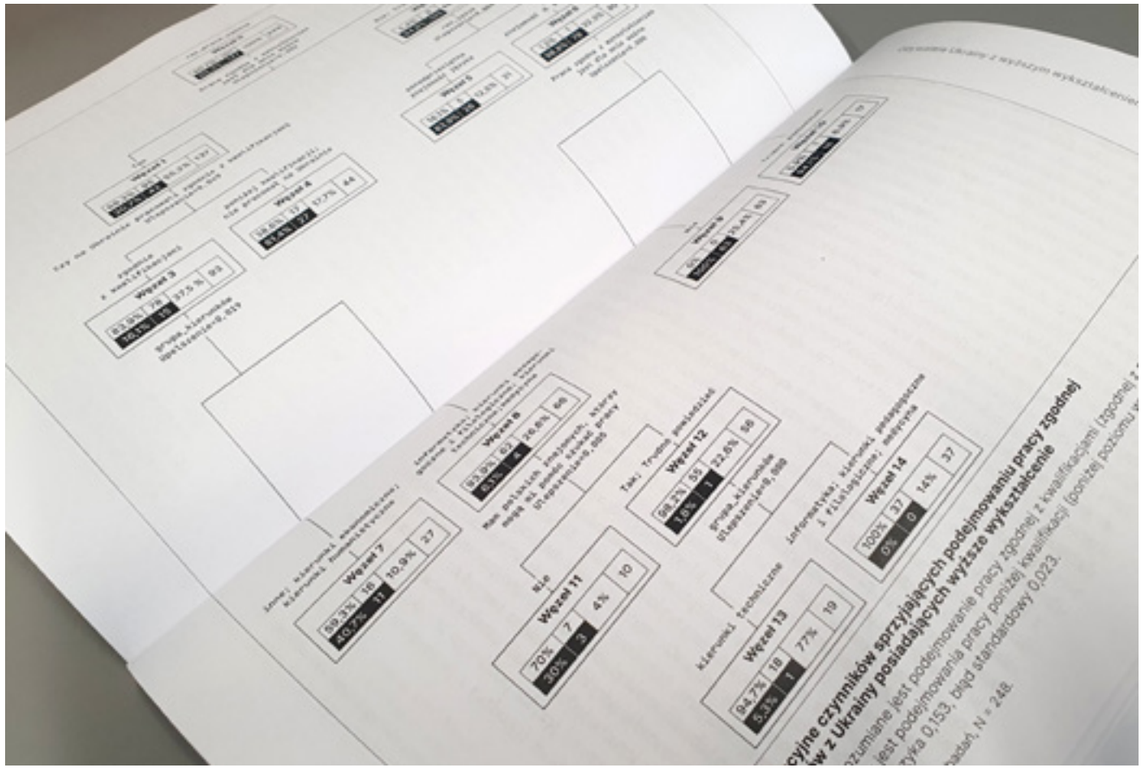
* Wykres przedstawia rozkład w
lę Likerta. W przypadku nie
wadzać pewne ograniczen
udziały procentowe, aby

Źródło: Opracowanie w

W badane
rem z



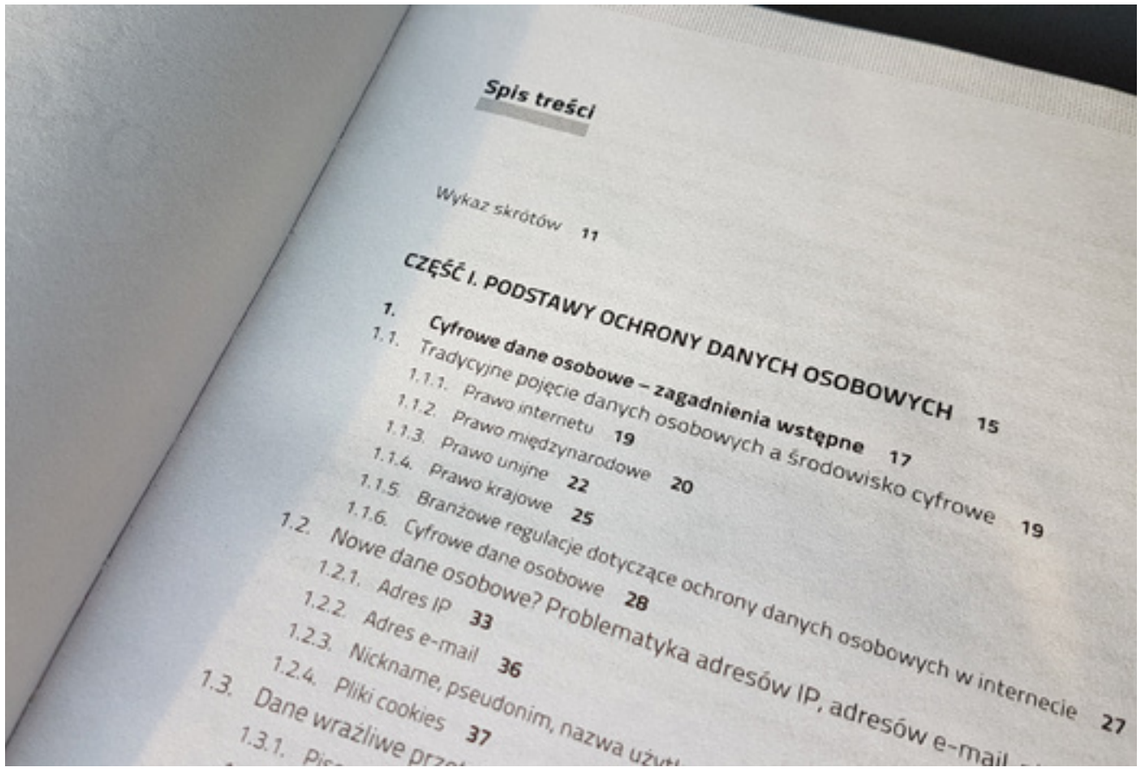




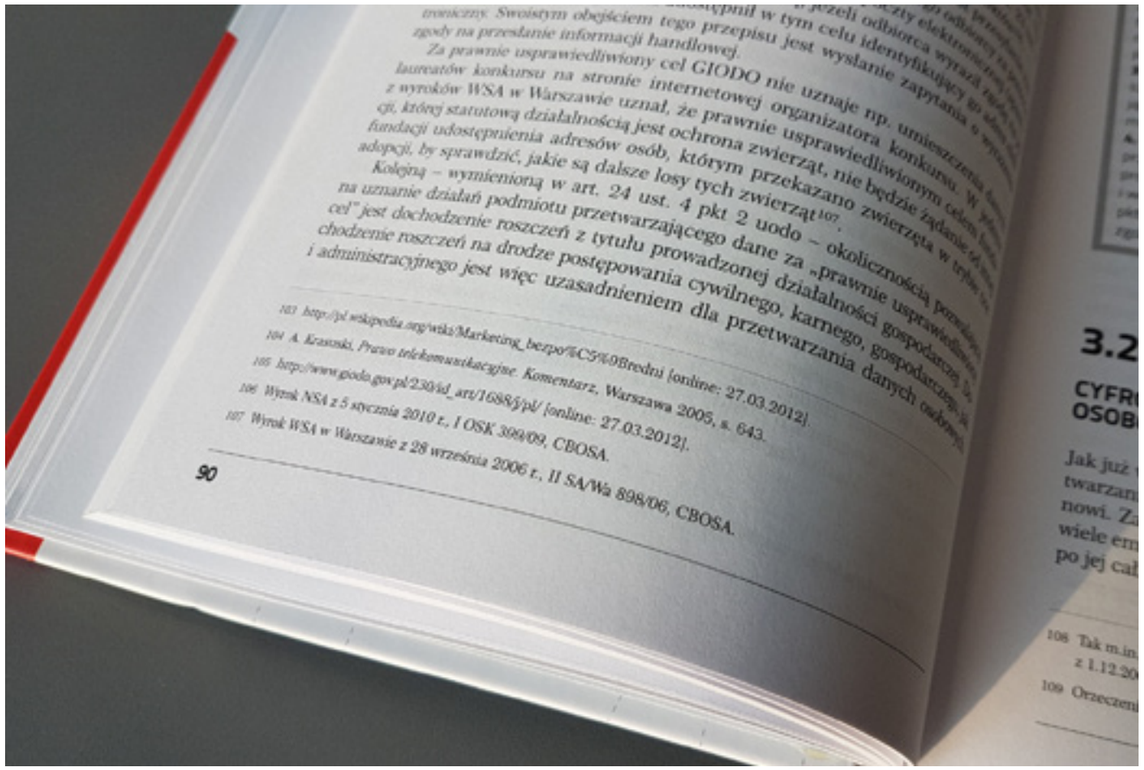
09. Book #3 – design and typography

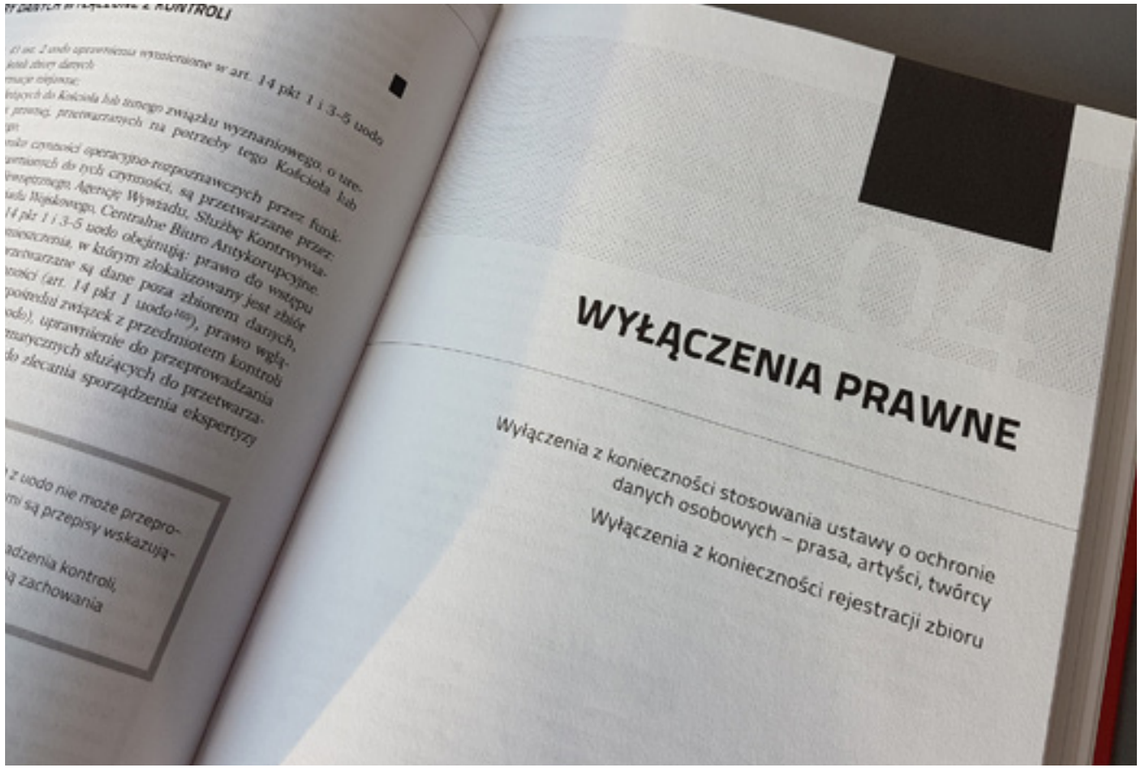
Scope of work:
– design
– layout
– typography
– desktop publishing
– pre-press

↑ Click to move to Table of Contents



Spis treści



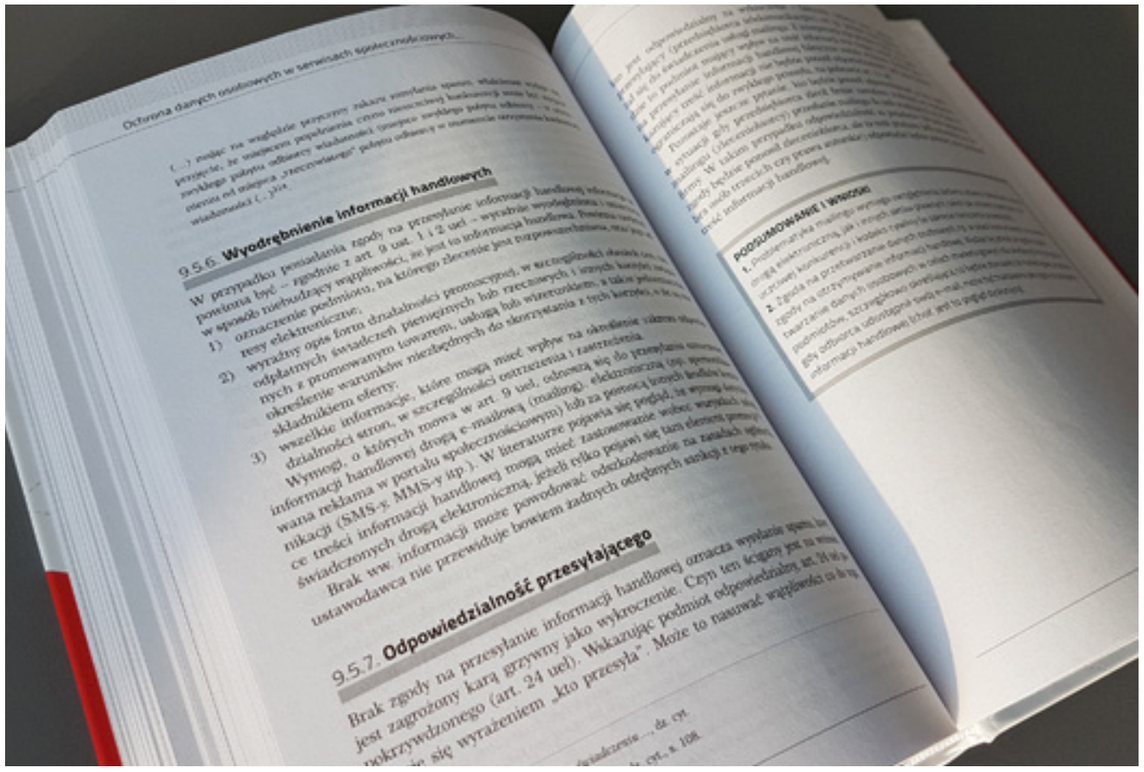


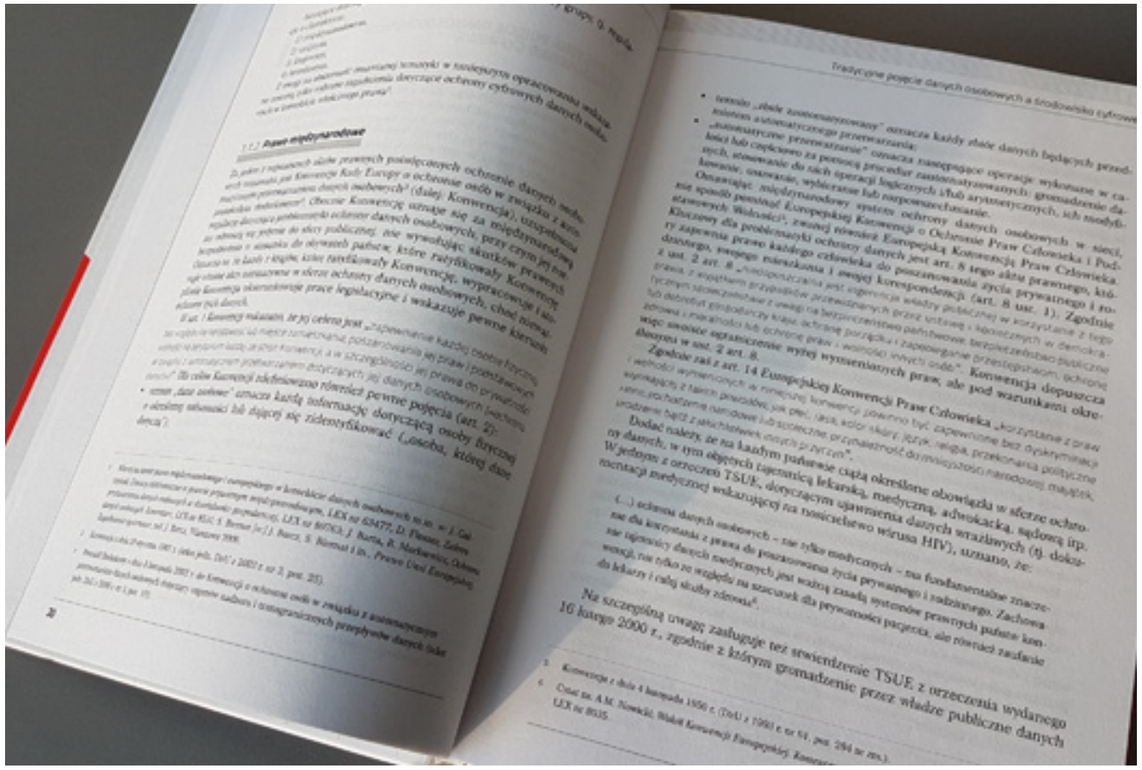
WYŁĄCZENIA PRAWNE

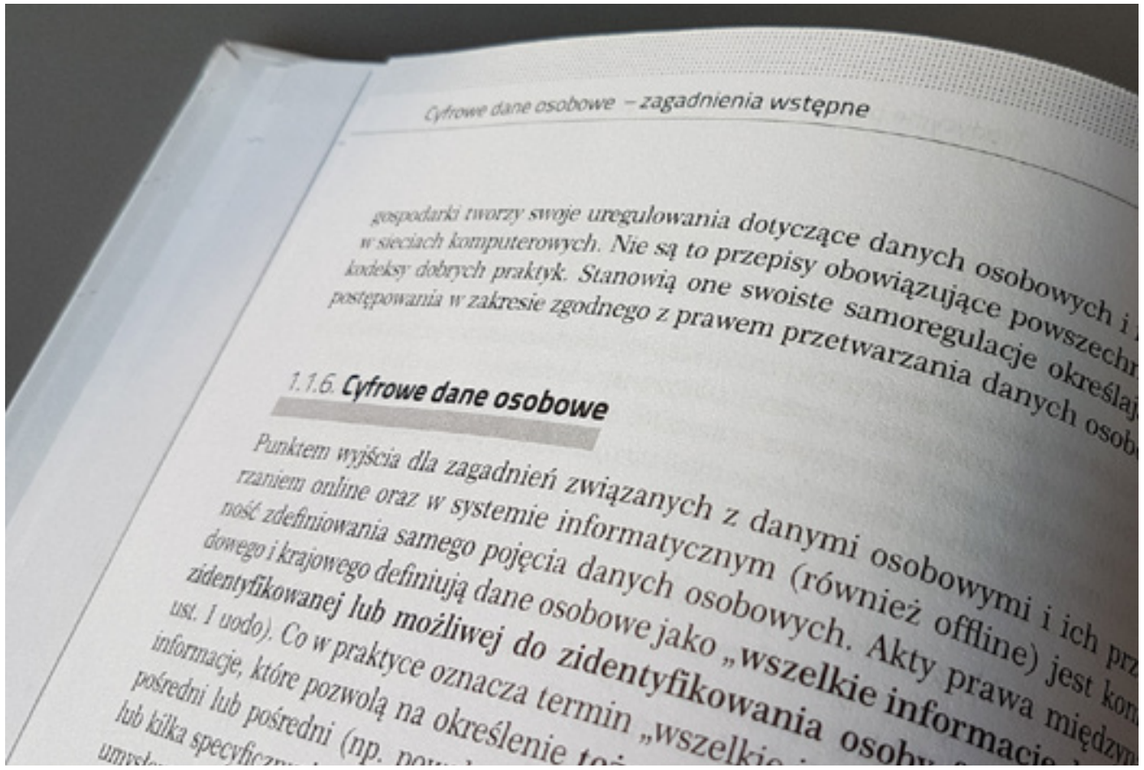
Wyłączenia z konieczności stosowania ustawy o ochronie danych osobowych – prasa, artyści, twórcy

Wyłączenia z konieczności rejestracji zbioru


CZĘŚĆ III
DANE OSOBOWE
W ADMINISTRACJI PUBLICZNEJ


Ochrona danych osobowych w serwisach społecznościowych
9.5.6. Wyodrębnienie informacji handlowych
9.5.7. Odpowiedzialność przesyłającego
PODSUMOWANIE I WNIOSKI


Tradycyjne pojęcie danych osobowych a środowisko cyfrowe

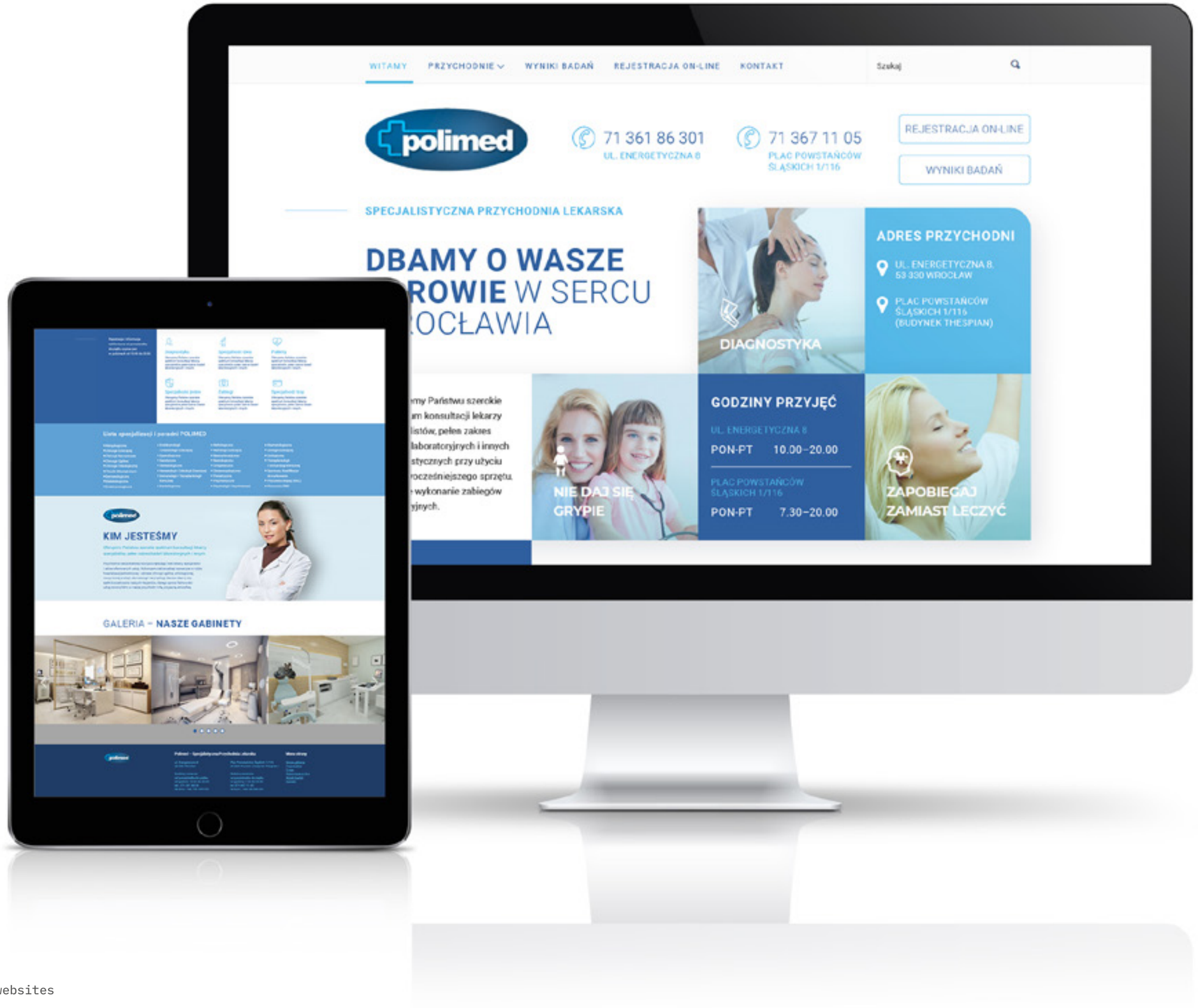

Cyfrowe dane osobowe – zagadnienia wstępne
1.1.6. Cyfrowe dane osobowe

10. Websites

Scope of work:
– design
– typography
– UX/UI
– coding and programming
– CMS and e-commerce integration
– add-on systems such as encryption of purchased ebooks, paid access and membership system, forms and surveys

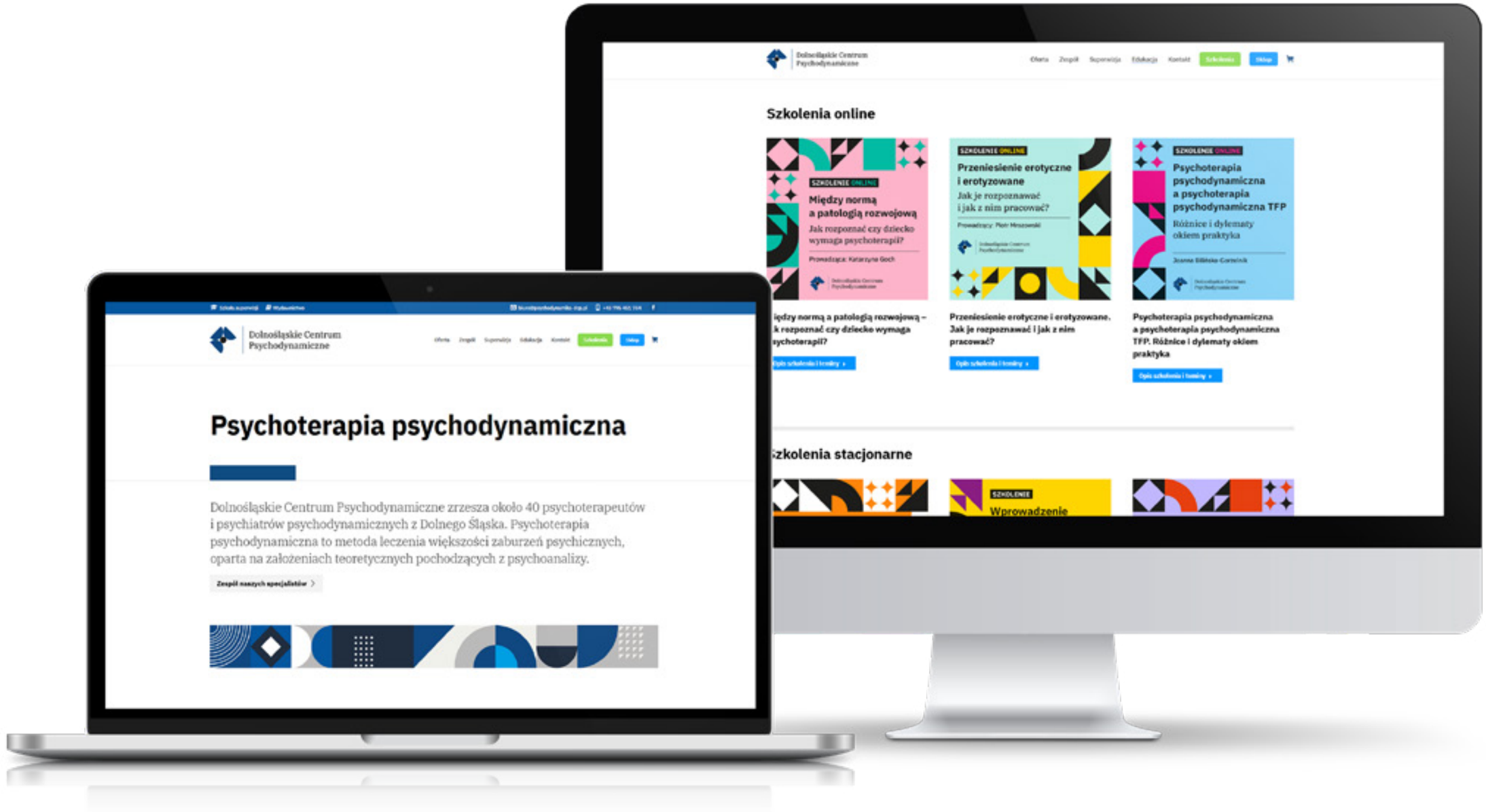
↑ Click to move to Table of Contents

Examples of websites

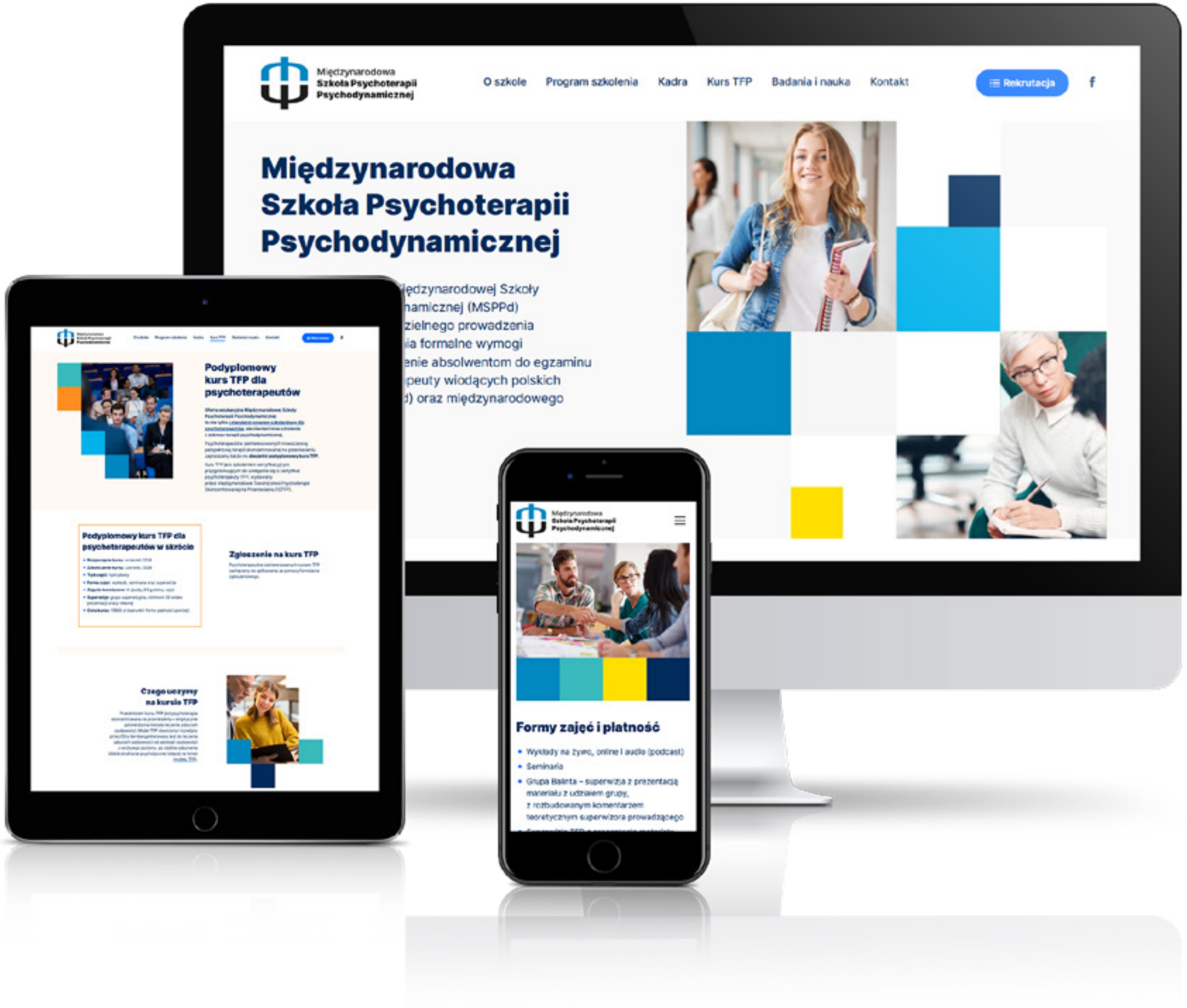


Examples of websites


LIPALI
WITAMY BIO NEWSY KONCERTY DYSKOGRAFIA KONTAKT SKLEP
ZAMÓW PŁYTĘ BEZPOŚREDNIO OD ZESPOŁU!
Odwiedź nas!
NAJBLIŻSZE KONCERTY
TERMIN MIEJSCE BILETY
29 listopada 2015
5 grudnia 2015
6 grudnia 2015
WSTĘP WOLNY
NEWSY
POMÓŻ DZIECIOM I SENIOROM – POWIEŚ LIPĘ NA ŚCIANIE!
PREORDER
„FASADY" JUŻ W PRZEDSPRZEDAŻY
FASADY [2015]
DO ZOBACZENIA NA KONCERTACH
OSTATNIE NEWSY


Dolnośląskie Centrum Psychodynamiczne
Oferta
Zespół
Superwizja
Edukacja
Kontakt
Szkolenia
Sklep
Psychoterapia psychodynamiczna
Dolnośląskie Centrum Psychodynamiczne zrzesza około 40 psychoterapeutów i psychiatrów psychodynamicznych z Dolnego Śląska. Psychoterapia psychodynamiczna to metoda leczenia większości zaburzeń psychicznych, oparta na założeniach teoretycznych pochodzących z psychoanalizy.
Zespół naszych specjalistów
Szkolenia online
SZKOLENIE ONLINE
Między normą a patologią rozwojową
Jak rozpoznać czy dziecko wymaga psychoterapii?
Prowadząca: Katarzyna Goch
Przeniesienie erotyczne i erotyzowane
Jak je rozpoznawać i jak z nim pracować?
Psychoterapia psychodynamiczna a psychoterapia psychodynamiczna TFP
Różnice i dylematy okiem praktyka
Przeniesienie erotyczne i erotyzowane. Jak je rozpoznawać i jak z nim pracować?
Psychoterapia psychodynamiczna a psychoterapia psychodynamiczna TFP. Różnice i dylematy okiem praktyka
Opis szkolenia i terminy
Szkolenia stacjonarne
SZKOLENIE
Wprowadzenie


udane wycieczki
Szczególnie polecamy
udane wycieczki
Najnowsze artykuły i recenzje


Międzynarodowa
Szkoła Psychoterapii
Psychodynamicznej
O szkole
Program szkolenia
Kadra
Kurs TFP
Badania i nauka
Kontakt
Rekrutacja
Międzynarodowa Szkoła Psychoterapii Psychodynamicznej
Podyplomowy kurs TFP dla psychoterapeutów
Podyplomowy kurs TFP dla psychoterapeutów w skrócie
Zgłoszenie na kurs TFP
Czego uczymy na kursie TFP
Formy zajęć i płatność
Wykłady na żywo, online i audio (podcast)
Seminaria
Grupa Balinta – superwizja z prezentacją materiału z udziałem grupy, z rozbudowanym komentarzem teoretycznym superwizora prowadzącego


Nowoczesne technologie


EAVPT
About EAVPT
Membership
Research
History
Contact
EAVPT Congress 2022 in Lviv
EAVPT RESEARCH
Our scientific community is engaged in a broad spectrum of research in the basic and clinical aspects of veterinary pharmacology and toxicology employing in vitro, in vivo, ex vivo or in silico models
EAVPT officially supports the Journal of Veterinary Pharmacology and Therapeutics (JVPT) as our primary arena for exchange of thoughts and publication of research. The books of abstracts of the EAVPT Congresses are traditionally published as JVPT supplements.
EAVPT AS GLOBAL ORGANISATION
52
countries around the world
41
years of activity
EUROPEAN ASSOCIATION FOR VETERINARY PHARMACOLOGY AND TOXICOLOGY
The European Association for Veterinary Pharmacology and Toxicology is an association that promotes the disciplines of veterinary pharmacology, toxicology and therapeutics.
EDUCATION AND RESEARCH
EAVPT aims to promote education and research in the fields of veterinary pharmacology and toxicology. It achieves these aims through organizing congresses, workshops, symposia or other scientific and educational meetings. In addition, EAVPT enhances the exchange of education materials, ideas and teachers between veterinary institutes.
COMMITTEES OF EXPERTS
EAVPT organizes committees of experts to make recommendations on current problems in veterinary pharmacology, toxicology and therapeutics, including concerns in relation to human and environmental health. EAVPT has members from around the world and hosts an international congress every 3 years – with the next congress planned for 2022 – more.


SAHC 2012
8th International Conference on Structural Analysis of Historical Constructions
Welcome
News
Topics
Committees
Patronage
Conference venue
Registration Form
Accommodation
Proceedings
Sponsors
Contact
Organizers:
Co-Organizers
Key dates


Oficjalna strona zespołu Illusion
illusion
WITAMY
NEWSY
KONCERTY
BIO
DYSKOGRAFIA
ZDJĘCIA
VIDEO
KONTAKT
SKLEP
WITAMY!
Nowa strona, nowa płyta, nowa trasa koncertowa
ZAMÓW PŁYTĘ BEZPOŚREDNIO OD ZESPOŁU!
TRASA KONCERTOWA
ZDJĘCIA
ZDJĘCIA
WARSZAWA - STUDIO IM. AGNIESZKI OSIECKIEJ
KATOWICE - EMPIK SILESIA MEGASTORE
ZABRZE - CK WIATRAK (2014)
KRAKÓW - KLUB STUDENCKI KWADRAT
KATOWICE - MEGACLUB (2014)
WARSZAWA - TORWAR (2011)


VETOS FARMA
O NAS
PRODUKTY
LUDMUŻORIA
PRODUKCJA KONTRAKTOWA
KONTAKT
Sklep
Polski producent leków i preparatów weterynaryjnych
Poznaj nasze produkty
Cztery filary naszej działalności
Skuteczne i ekonomiczne leki i preparaty witaminowe


Łączymy naukę, technologię i nowoczesną produkcję w trosce
o nas i środowisko w którym żyjemy
VETOS-FARMA
Szeroka gama preparatów weterynaryjnych
Produkujemy skuteczne i ekonomiczne leki i preparaty witaminowe, które wspomagają prawidłowy rozwój i zdrowie zwierząt hodowlanych. W ofercie mamy również bogaty wybór wysokiej jakości preparatów dla zwierząt towarzyszących oraz produkty zootechniczne.
Przejdź na stronę marki VETOS-FARMA
VMED
Certyfikowane produkty lecznicze i pielęgnacyjne
Produkujemy produkty lecznicze i pielęgnacyjne, a także środki dezynfekcyjne, którym można zaufać. Główny Inspektorat Farmaceutyczny przyznał nam certyfikat GMP. Gwarantuje on kontrolę jakości i przebiegu produkcji produktów leczniczych przeznaczonych dla ludzi.
Przejdź na stronę marki VMED
e i skuteczne
raty odchudzające


VETOS FARMA
GRUPA VETOS-FARMA
WITAMY
O FIRMIE
AKTUALNOŚCI
CERTYFIKATY GMP
KATALOG
SKLEP
KARIERA
KONTAKT
Laboratorium
Weterynaria
Laboratorium
Farmacja
Weterynaria
Weterynaria
Leki i preparaty witaminowe
Preparaty dla zwierząt towarzyszących
Produkty zootechniczne

Thank you for watching!

Feel free to invite me to:

CONTACT

Marcin Szewczyk-Wilgan – full-stack designer

marcin.szewczyk@m4c.pl

+48 608 271 665

Wrocław, Poland