General Data Protection Regulation

- GDPR = General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
- Školící materiál pro poradce

Modrá pyramida

OBSAH

Modrá pyramida

I. GDPR = General Data Protection Regulation

EVROPSKÉ OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ č. 2016/679

- Účinnost od 25.5.2018
- Vztahuje se na zpracování osobních údajů všech fyzických osob, vč. podnikatelů (FOO, FOP)
- Nevztahuje se na údaje právnických osob, anonymizované údaje, údaje o zemřelých osobách

CÍLE

- Harmonizovat pravidla ochrany osobních údajů v rámci EU
- Posílit práva osob (zaměstnanců, klientů, potenciálních klientů,…) a odpovědnost organizací

NÁRODNÍ ADAPTAČNÍ ZÁKONY

- Český - 110/2019 Sb., Zákon o zpracování osobních údajů, platnost od 24.4.2019

REGULÁTOR

- Regulátorem v ČR je Úřad pro ochranu osobních údajů (www.uoou.cz)
- Na úrovni EU je vrchním regulačním orgánem Evropský sbor pro ochranu osobních údajů – European Data Protection Board (EDPB)

SANKCE

- Až 20 mil EUR nebo 4% celosvětového ročního obratu

II. Pro koho je určeno ?

- Vztahuje se na zpracování osobních údajů **Fyzických osob (FO)** a **fyzických osob podnikatelů (FOP).**
- Platí, **i kdekoli na světě** pokud jsou zpracovávány osobní údaje občanů EU.
- Je **závazné pro všechny, kdo zpracovávají osobní údaje na území EU** např.: banky, finanční instituce, obchodníci, e-shopy, provozovatelé webových stránek, sociální sítě, státní správa, nemocnice, obecní úřady, lékaři, zdravotní pojišťovny, finanční úřady,..

Modrá pyramida

III. Základní pojmy

SUBJEKT ÚDAJŮ

- jakákoliv fyzická osoba v nejrůznějších životních situacích nebo vztazích např. já, vy, vaše rodina, zákazníci zaměstnanci, pojištěnci, pacienti, občané…….

OSOBNÍ ÚDAJ

- veškeré informace o identifikovaném nebo identifikovatelném subjektu údajů, bez ohledu na to, jestli je o sobě poskytnul sám, pocházejí z jiného zdroje, nebo jsme si je sami vytvořili: jméno, příjmení, datum narození, rodné číslo, adresa, číslo průkazu totožnosti, telefonní číslo, e-mailová adresa, IP adresa, číslo účtu, identifikační číslo, věk, pohlaví, rodinný stav, vzdělání, informace o užívaných produktech ...
- **zvláštní kategorie osobních údajů (tzv. citlivé údaje**): zdravotní stav, genetické údaje, biometrické údaje, rasový či etnický původ, politické názory, náboženské vyznání, členství v odborech, sexuální orientace. . Zpracování citlivých údajů podléhá přísnějšímu režimu, než je tomu u obecných údajů, a proto doporučujeme **nezapisovat a neevidovat tyto osobní údaje, pokud to není nezbytně nutné**!

SPRÁVCE (= Modrá pyramida)

- určuje účely a prostředky zpracování osobních údajů a je je zodpovědný za řádné a zákonné zpracování osobních údajů

Modrá pyramida

Základní pojmy

- ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ = jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je:

  - shromáždění
  - zaznamenání
  - uspořádání,
  - strukturování
  - uložení
  - přizpůsobení nebo pozměnění
  - vyhledání
  - nahlédnutí
  - použití
  - zpřístupnění přenosem
  - šíření nebo jakékoliv jiné zpřístupnění
  - seřazení či zkombinování
  - omezení
  - výmaz nebo zničení

I to, že údaje někde leží v databázi a na nic je nepoužíváme.

Modrá pyramida

Základní pojmy

- ZPRACOVATEL = **fyzická nebo právnická osoba**, orgán veřejné moci, agentura nebo jiný subjekt, který **zpracovává osobní údaje pro správce**.

Zpracovatelem je dodavatel MP, který pro MP mj. zpracovává osobní údaje jejích klientů, zaměstnanců, finančních poradců…..Zpracovatelem je i např. finanční poradce.

Zákonné tituly : (důvod proč zpracovávám osobní údaje)

Osobní údaje nemůže nikdo zpracovávat jen tak, protože se mu to zlíbí, můžou se hodit, jsou prostě dostupné, zjednoduší mu práci, nebo by je mohl zpeněžit!

Osobní údaje mohu zpracovávat pouze pokud k tomu mám jeden ze **zákonných titulů**, které stanoví GDPR. např: Plnění **smlouvy** / jednání o uzavření smlouvy, nebo **Splnění právní povinnosti správce**, nebo Účely **oprávněných zájmů** příslušného správce či třetí strany…..a jiné

Modrá pyramida

IV. Zpracování osobních údajů

PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ JE NUTNO:

- nakládat s osobními údaji tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům či k jejich jinému neoprávněnému zpracování a **zpracovávat tyto údaje pouze v souladu s účelem stanoveným** a nepoužít je způsobem, jenž by byl v rozporu se zájmy subjektu údajů, MP nebo smluvního partnera MP.

- **dbát, aby subjekt údajů neutrpěl újmu na svých právech**, zejména na právu na zachování lidské důstojnosti, a dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

- **neposkytovat zpracovávané osobní údaje třetím osobám**. To neplatí, děje-li se tak v souladu s právními předpisy na ochranu osobních údajů, zejména GDPR, a byl-li k tomu zpracovateli udělen výslovný souhlas ze strany MP a subjektu údajů. Zpracovatel se zavazuje zajistit, že osoby, které pro něj zpracovávají osobní údaje, jsou pravidelně řádně proškolovány ohledně povinností souvisejících se zpracováním osobních údajů.

Modrá pyramida

V. Práva subjektu údajů = Práva klienta

1) **Transparentní informace** – právo být informován jednoduchým a srozumitelným způsobem (Informační memorandum)
2) Právo na **přístup** k osobním údajům – výpis zpracovávaných údajů
3) Právo na **opravu** osobních údajů – právo opravovat či doplňovat osobní údaje
4) Právo na **výmaz** osobních údajů – právo být zapomenut
5) Právo na **omezení** zpracování osobních údajů – právo omezit zpracování po dobu řešení opravy či námitky nebo pokud nechce výmaz
6) Právo na **přenositelnost** údajů – právo získat informace ve strukturovaném, běžné používaném a strojově čitelném formátu
7) Právo na **námitku** proti zpracování osobních údajů – právo vznést námitku proti zpracování na základě oprávněného zájmu nebo přímého marketingu
8) Právo **nebýt předmětem automatizovaného rozhodování** – právo subjektu údajů nebýt předmětem rozhodnutí založeném výhradně na automatizovaném zpracování
9) **Odvolání souhlasu** – právo na odvolání poskytnutého souhlasu se zpracováním osobních údajů
10) **Stížnost** u dozorového úřadu – právo podat stížnost u úřadu pro ochranu osobních údajů

Modrá pyramida

VI. Klientský souhlas - oslovování

- KOHO OSLOVUJEME?
- **Všechny stávající Klienty** (FO, FOP)
- **Nové Klienty** nabízíme podpis marketingového souhlasu **VŽDY**

- KOMUNIKAČNÍ DESATERO PRO ZÍSKÁNÍ MARKETINGOVÉHO SOUHLASU (GDPR):

1. Finanční poradce zná / má nastudované znění obou dokumentů: **Marketingový souhlas a Informace o zpracování osobních údajů**
2. Férová a otevřená komunikace s klientem je základ
3. Před sběrem nového souhlasu byste měli vědět o tom starém
4. Není vhodné aktivně oslovovat klienta a zvát jej na obchodní schůzku pouze kvůli marketingovému podpisu
5. Udělení souhlasu není pro nikoho povinné – je zcela dobrovolné. Podpis souhlasu nesmí být vynucován či podmiňován
6. Udělení / neudělení souhlasu nemá vliv na používání služeb, produktů, ani klientský servis
7. Udělení / neudělení souhlasu má vliv pouze na marketing a sdílení ve skupině KB/SG
8. Každému klientovi musí být vždy nabídnut a vysvětlen obsah dokumentu „Informace o zpracování osobních údajů“. Na vlastní žádost si jej může i před podpisem odnést
9. Každý klient musí být informován o možnostech souhlas udělit, neudělit, nevyjádřit se k němu či jej odvolat
10. Poskytujte jen přesné a ověřené informace, a když si nevíte rady, ptejte se

Modrá pyramida

Klientský souhlas - argumentace

POVOLENÉ (DOPORUČENÉ) ARGUMENTY

👍 **Udělením** Marketingového Souhlasu **umožníte**, abychom Vás informovali o nových či výhodnějších produktech a službách celé skupiny

👍 **Udělením** Marketingového Souhlasu nám **umožníte** vyhodnotit, zdali jsou produkty, které máte aktuálně nastavené dostačující. Abychom Vám případně mohli nabídnout jinou alternativu

👍 Vzhledem k tomu, že jste Souhlas s poskytováním osobních údajů pro marketingové účely v minulosti poskytl/a, prakticky nic se pro Vás podpisem nového souhlasu nemění **a nemusíte se obávat žádných negativních změn** – pozn. tento argument je možné použít pouze v případech, kdy jste schopni zjistit, že má klient předchozí Souhlas se zpracováním osobních údajů udělen.

👍 Kvůli nové regulaci EU (GDPR) přestává Váš dosavadní souhlas 25. 5. 2018 platit. Abychom i nadále mohli Vaše údaje pro marketingové účely zpracovávat, **potřebujeme jenom aktualizovat Váš souhlas**. Nový souhlas přitom splňuje přísnější požadavky EU regulace, zmenšuje počet společností, kterým souhlas udělujete a zpřesňuje rozsah zpracovávaných údajů – POZN. tento argument je možné použít pouze v případech, kdy jste schopni zjistit, že má klient předchozí Souhlas se zpracováním osobních údajů udělen.

ZAKÁZANÉ ARGUMENTY

👎 EU nám nařizuje sbírat nový souhlas.

👎 Kvůli EU nám musíte dát nový souhlas.

👎 Když nám souhlas nepodepíšete, tak Vám nemůžeme dát informace o vašich produktech.

👎 „Neuvidíme“ na Vás a Vaše produkty.

👎 Ztížíte si komunikaci s Vámi.

👎 Nebudeme Vám moci nabídnout naše produkty, ani když si o ně sami řeknete.

Modrá pyramida

Klientský souhlas – změny v eKmeni

ZOBRAZOVÁNÍ EXISTENCE MARKETINGOVÉHO SOUHLASU (GDPR) A INFORMATIVNÍCH HLÁŠEK V EKMENI:

1. **Klient udělil souhlas a ten je v platné verzi**

   ANO – Klienta oslovujte s nabídkami MP nebo nabídkami dalšího člena finanční skupiny KB/SG.
   Klienta můžete oslovovat v rámci tzv. "péče o klienty" (např. dotazy na spokojenost).

2. **Klient udělil souhlas ve starší verzi, tj. již existuje a platí novější verze souhlasu**

   ANO, STARŠÍ VERZE - Starší verze souhlasu, při jednání s klientem požádejte klienta o aktualizaci souhlasu.

3. **Klient odmítl udělit souhlas, nebo ho odvolal**

   NE - Klienta neoslovujte s žádnými nabídkami, ani v rámci tzv. "péče o klienta" (např. dotazy na spokojenost).
   - **Případně pokud bude mít evidován příznak “Požadavek na oslovení”**

   NE - Klienta neoslovujte s žádnými nabídkami, ani v rámci tzv. "péče o klienta" (např. dotazy na spokojenost). Při jednání můžete klienta o udělení souhlasu požádat.

4. **Klient se zatím nevyjádřil nebo jeho souhlas již expiroval**

   BEZ VYJÁDŘENÍ - Klienta neoslovujte s žádnými nabídkami, ani ho o udělení souhlasu nežádejte (proběhlo v nedávné době).
   - **Případně pokud bude mít evidován příznak “Požadavek na oslovení”**

   Klienta neoslovujte s žádnými nabídkami, při jednání požádejte klienta o udělení souhlasu.

Modrá pyramida

Klientský souhlas - obrazovky v eKmeni

Poznámka: jedná se o obrazovky z testovacích verzí aplikací, které mohou být ještě upravovány a mohou se tak odlišovat od produkčních verzí.

Modrá pyramida

VII. Řešení práv subjektů údajů - proces

1.OVĚŘIT SUBJEKT

- Ověřit (identifikovat) subjekt dle standardních pravidel identifikace v MP (např. Občanský průkaz)

2.VYPLNIT ŠABLONU ŽÁDOSTI O VÝKON PRÁV SUBJEKTU (VPS)

- Vyplnit šablonu Žádosti o VPS a zvolit některé z následujících práv a blíže specifikovat:

1) Výpis údajů

- Subjektu bude poskytnut seznam evidovaných osobních údajů v tiskové podobě

2) Portabilita - přenositelnost údajů

- Subjektu budou poskytnuty jeho osobní údaje v elektronické podobě
- V sekci „BLIŽŠÍ SPECIFIKACE POŽADAVKU“ bude možno upřesnit, zda-li požaduje data:
  a) Poštou - obdrží na kompaktním disku (CD) nebo
  b) E-mailem - zaslat zašifrovaně na uvedený kontaktní e-mail v Žádosti (heslo obdrží SMS zprávou)

3) Oprava osobních údajů

- Subjektu bude umožněno opravit jeho osobní údaje

☝ U požadavků na odvolání Marketingového souhlasu či změny kontaktních / identifikačních údajů využívejte standardní šablony, které jsou pro tyto účely určeny (šablony 0410 a 1003)

☝ U požadavku na opravu jiných údajů je nutno specifikovat, o jaké údaje se jedná

Modrá pyramida

Řešení práv subjektů údajů - proces

4) Výmaz osobních údajů

- Subjektu bude umožněno požadovat výmaz osobních údajů, pokud již MP nemá žádný zákonný titul, oprávněný zájem nebo marketingový souhlas pro využívání těchto osobních údajů

5) Omezení zpracování / Námitka ke zpracování

- Subjekt bude moci vznést námitku na omezení zpracování, která bude individuálně posouzena a vyhodnocena z pohledu oprávněnosti

6) Automatizované rozhodování

- Subjekt bude moci vznést námitku k automatizovanému rozhodování a profilaci, která bude individuálně posouzena a vyhodnocena z pohledu oprávněnosti

4.VYPLNĚNOU ŽÁDOST ODESLAT POŠTOU NA CMP NEBO NASKENOVANOU NA SCHRÁNKU podatelna@mpss.cz

a) Odeslat Žádost poštou na adresu: **Modrá Pyramida, Bělehradská 128, 120 21, Praha**, nebo je možno
b) Naskenovat Žádost a odeslat na emailovou adresu: podatelna@mpss.cz

5.ZPRACOVÁNÍ ŽÁDOSTI NA CMP A ODESLÁNÍ ODPOVĚDI SUBJEKTU DOPORUČENOU POŠTOU

1. Přijetí Žádosti na CMP a zpracování určenými odbornými útvary
2. Kompletace podkladů a odeslání doporučenou poštou subjektu na uvedenou kontaktní adresu v Žádosti o výkon práv subjektu

Modrá pyramida

Role finančního poradce

Role finančního poradce v procesu Žádosti o výkon práv subjektu (VPS):

Provádí pouze tyto kroky:

- 👍 Ověření a identifikace subjektu
- 👍 Vyplnění Žádosti o VPS a její postoupení na Centrálu Modré pyramidy ke zpracování
- 👍 Dodatečné ověření a identifikace subjektu
- 👍 Typický denní servis, kde klient požaduje opravu nebo změnu klientských údajů v systémech a nejedná se o výkon práv GDPR

V žádném případě neprovádí:

- 👎 Řešení žádosti
- 👎 Posouzení oprávněnosti žádosti
- 👎 Sestavování výstupní zprávy
- 👎 Zjišťování, v jakém vztahu je subjekt k MP (zaměstnanec, bývalý zaměstnanec, finanční poradce, dodavatel toto provádí CMP)

Modrá pyramida

Typové situace

1. **Klient požaduje opravu kontaktního telefonu nebo adresy nebo jiného osobního údaje v systémech MP**

- Provádí finanční poradce v rámci běžného servisu vyplňuje formulář (1003) - zde je finanční poradce sám řešitelem
- Pokud však klient opravovaný údaj rozporuje, reaguje negativně a požaduje informaci, jak a kde banka k tomuto údaji přišla, pak se jedná o Výkon Práv Subjektu (VPS) a finanční poradce svou aktivní roli končí a pouze zasílá žádost o VPS na CMP ke zpracování

2. **Na poradenské centrum přichází žadatel (tj. jakákoliv fyzická osoba, např. i bývalý zaměstnanec) a požaduje výpis osobních údajů, které o něm vedeme**

- Finanční poradce provede identifikaci na základě dokladu totožnosti (dle standardních pravidel Modré knihy MP), vyplní a zasílá žádost o VPS na CMP ke zpracování
- Finanční poradce nezkoumá, jaká data o této osobě vedeme, pouze postoupí žádost na CMP
- CMP po zpracování posílá odpověď, která je formou standardizovaných šablon a jejich příloh

Modrá pyramida

GDPR incidenty

CO ZNAMENÁ POJEM „GDPR INCIDENT“?

Jedná se o **incidenty**, které vedou k náhodnému nebo **protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů fyzických osob.**

KDY VZNIKÁ INCIDENT?

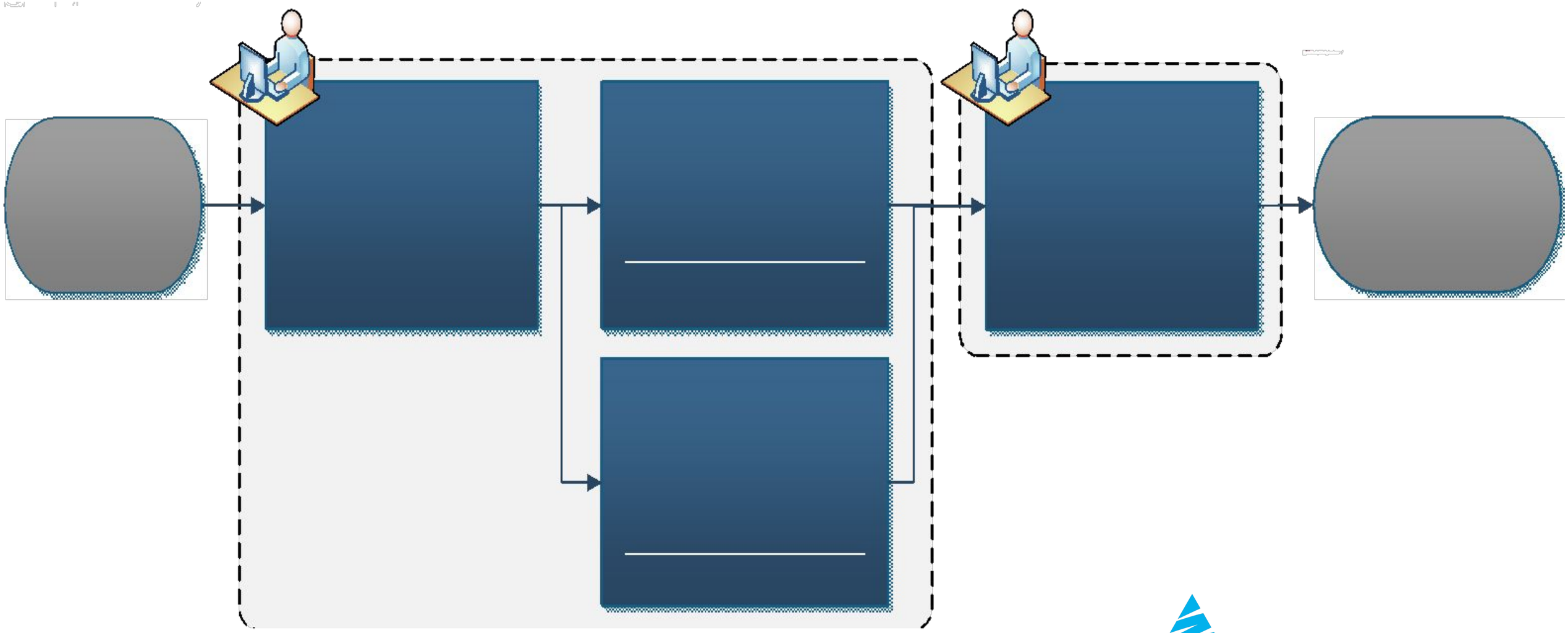
Vzniká v okamžiku, kdy se banka dozví (respektive kdy bylo vyhodnoceno), že došlo k porušení zabezpečení osobních údajů
Od této chvíle má banka lhůtu „**do 72 hodin**“, do kdy musí **incident ohlásit přes DPO KB** (Data Protection Officer = pověřenec na ochranu dat v Komerční bance) **na příslušný úřad**, že došlo k porušení zabezpečení osobních údajů

PŘÍKLADY INCIDENTŮ

- Chybný adresát - klient obdržel výpis jiného klienta a informuje svého finančního poradce
- Porušení bankovního tajemství
- Ztráta nebo odcizení tištěných dokumentů s osobními údaji (klientských smluv) na poradenském centru nebo jejich chybná likvidace
- Neoprávněný přístup třetích osob k osobním údajům klienta, jejich zničení nebo změna
- Ztráta nebo odcizení notebooku, PC, mobilního zařízení, externího disku obsahující osobní údaje klientů
- Napadení počítače s osobními údaji klientů škodlivým kódem nebo útočníkem

Modrá pyramida

Proces – porušení zabezpečení osobních údajů



Modrá pyramida

VIII. Desatero doporučení + 1 bonus

- **ZKONTROLUJ** dvakrát adresáty (komu je zpráva určena) před odesláním emailové zprávy.
- **PRO EMAILOVOU KOMUNIKACI** mezi poradcem a klientem/potenciálním klientem je povoleno z důvodu bezpečnosti a ochrany osobních údajů používat pouze firemní mail Modré pyramidy „jméno@mpss.cz“.
- **CHRAŇ** elektronicky přenášená data (zejména mimo informační síť MP) pomocí šifrování (např. zip + heslo).
- **DODRŽUJ** pravidlo čistého stolu.
- **UCHOVÁVEJ** dokumenty s daty, ale i přenosná média apod. na zabezpečeném místě - pod uzamčením.
- **VYZVEDNI** si vytištěné dokumenty s citlivými / důvěrnými daty co nejdříve z tiskárny.
- **SKARTUJ** nepotřebné dokumenty s citlivými / důvěrnými daty, nebo je vhoď do speciálního kontejneru.
- **VYMAŽ** data z přenosných médií po použití.
- **NEUKLÁDEJ** citlivé *(např. zdravotní stav, náboženské vyznání, atp.)* nebo důvěrné osobní údaje do různých Poznámek, vlastních evidencí nebo na Internetová cloudová úložiště, která nejsou MP schválena.
- **ZAMKNI** PC/NTB (pomocí CTRL+ALT+DEL a ENTER) před jeho opuštěním – zamez tomu, aby se dovnitř dostala nepovolaná osoba.

Modrá pyramida

VIII. Desatero omylů

- Odeslání emailové zprávy s důvěrnými daty **NESPRÁVNÉMU ADRESÁTOVI A NEBO Z JINÉHO NEŽ FIREMNÍHO MAILU @mpss.cz** (hromadné rozeslání zprávy s důvěrnými daty o klientech všem klientům).
- **NEZAŠIFROVÁNÍ, NEZAHESLOVÁNÍ** souboru s důvěrnými daty.
- **HROMADNÉ ROZESLÁNÍ** emailové zprávy klientům, kdy adresáti/klientské emailové adresy nejsou ve „**SKRYTÁ KOPIE**“, ale v „Komu“.
- Likvidace dokumentace s osobními údaji pouhým vhozením **DO POPELNICE BEZ SKARTACE.**
- Mylná představa, že na osobní údaj získaný **Z VEŘEJNÝCH ZDROJŮ** (jinak než od klienta) se nevztahuje režim ochrany osobních údajů GDPR.
- **VEDENÍ VLASTNÍHO SEZNAMU KONTAKTŮ / ÚDAJŮ** a jejich neaktualizování a následné použití pro poskytování finančního poradenství.
- Předání údajů **DALŠÍ OSOBĚ**; sdělení citlivých informací osobě, která je např. **S KLIENTEM SPŘÍZNĚNA**, ale není to zákonný zástupce klienta či účastník smlouvy.
- **PŘEDÁNÍ PŘÍSTUPOVÝCH ÚDAJŮ** (hesel) další osobě, která se tak může k údajům dostat.
- **NEDOSTATEČNÉ ZABEZPEČENÍ** dokumentů s citlivými údaji, případně jejich ztráta.
- Přístup finančního poradce / zaměstnance k **AUTORIZAČNÍM ÚDAJŮM KLIENTA** (např. stažení certifikátu klienta do

Modrá pyramida

Další informace

KDE NAJDU BLIŽŠÍ INFORMACE?

- **GDPR směrnice** https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016R0679
- **Intranet MP – GDPR obecně**: https://intranet.mpss.cz/Znalosti/klienti/Stranky/GDPR_obecne.aspx
  - GDPR INCIDENTY:
    - ✔ Seznámení
    - ✔ Šablona emailu na ohlášení GDPR Incidentu
  - VÝKON PRÁV SUBJEKTŮ ÚDAJŮ:
    - ✔ Seznámení
    - ✔ Šablona na výkon práv, včetně emailové verze
- **Interní směrnice** – Směrnice a pracovní postupy - 43 Právní

Modrá pyramida