Ing. Pavel SITTA
Odbor správy majetku MV

GDPR

GENERAL DATA PROTECTION REGULATION *(OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ)*

OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ, ZKRÁCENĚ ONOOÚ, PLNÝM NÁZVEM *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) Č. 2016/679 ZE DNE 27. DUBNA 2016 O OCHRANĚ FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ A O VOLNÉM POHYBU TĚCHTO ÚDAJŮ A O ZRUŠENÍ SMĚRNICE 95/46/ES (OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ)*, JE NAŘÍZENÍ EVROPSKÉ UNIE, JEHOŽ CÍLEM JE VÝRAZNÉ ZVÝŠENÍ OCHRANY OSOBNÍCH DAT OBČANŮ.

CÍLE ONOOÚ

- stanovuje pravidla ochrany fyzických osob v souvislosti se zpracováním jejich osobních údajů a pravidla pro pohyb osobních údajů.
- Nařízení chrání základní práva a svobody fyzických osob se zaměřením na právo ochrany osobních údajů.
- Volný pohyb osobních údajů v Evropské unii není z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů omezen ani zakázán.
- **Evropský sbor pro ochranu osobních údajů** přispívá k jednotnému uplatňování pravidel ochrany údajů v celé Evropské unii a prosazuje spolupráci mezi úřady pro ochranu osobních údajů v EU. Posláním je zajišťovat jednotné uplatňování obecného nařízení o ochraně osobních údajů a evropské směrnice o prosazování práva v Evropské unii. Může vydávat obecné pokyny k objasnění pojmů obsažených v evropských právních předpisech v oblasti ochrany údajů a poskytovat zúčastněným stranám jednotný výklad jejich práv a povinností.

OSOBNÍ ÚDAJ (ZVLÁŠTNÍ OSOBNÍ ÚDAJ)

- jméno a příjmení
- adresa
- telefonní číslo
- lokační údaje (např. funkce využívající údaje o poloze v mobilním telefonu)
- e-mailová adresa ve formátu jako např. jméno.příjmení@firma.cz
- Pohlaví (40 druhů pohlaví?)
- věk, datum a místo narození
- rasový nebo etnický původ
- osobní stav
- vzdělání
- zdravotní stav, sexuální život nebo sexuální orientace fyzické osoby
- genetické a biometrické údaje (DNA, krevní skupina, Rh faktor,…; snímek obličeje, otisk prstu, snímek sítnice nebo oční duhovky, podpis, hlas, …)
- příjem ze zaměstnání (mzda, plat), příjem z důchodu
- členství v odborech
- adresa IP (Internetový protokol)
- ID souboru cookie,
- identifikátor telefonu pro inzerenty
- fotografický, video a audio záznam,…

CO SE NEPOVAŽUJE ZA OSOBNÍ ÚDAJ

Jde především o následující:

- registrační číslo společnosti (IČO, DIČ, …)
- e-mailová adresa jako je například info@firma.com
- anonymizované údaje
- údaje o osobách zemřelých

OSOBNÍ ÚDAJ (ZÁKON Č. 110/2019 SB.,)

Zákon o ochraně osobních údajů

- osobní údaj = jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu
- citlivý osobní údaj = citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů

OSOBNÍ ÚDAJ (SMĚRNICE 95/46/ES A GDPR - N EP 2016/679)

Směrnice 95/46/ES

- osobní údaj = veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity

GDPR

- osobní údaj = veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

VĚCNÁ PŮSOBNOST ONOOÚ

Nařízení se vztahuje na automatizované zpracování osobních údajů i na neautomatizované zpracování osobních údajů obsažených v evidenci nebo těch, co mají být zařazeny do evidence.

Nařízení se nevztahuje na zpracování osobních údajů prováděné:

- při výkonu činností, které nespadají do oblasti působnosti práva Unie;
- členskými státy při výkonu činností, které spadají do oblasti působnosti hlavy V kapitoly 2 Smlouvy o EU (Společná zahraniční a bezpečnostní politika podléhá zvláštním pravidlům a postupům.);
- fyzickou osobou v průběhu výlučně osobních či domácích činností;
- příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.
- Zpracování osobních údajů orgány, institucemi a jinými subjekty Unie je upraveno mimo jiné nařízením (ES) č. 45/2001. Nařízení (ES) č. 45/2001 a další právní akty Unie týkající se takového zpracování osobních údajů jsou uzpůsobeny zásadám a pravidlům tohoto nařízení podle článku 98. Nařízením není dotčeno uplatňování směrnice 2000/31/ES **(„směrnice o elektronickém obchodu“).**

OSOBNÍ ÚDAJE (ONOOÚ)

- Nařízení zpřesňuje a rozšiřuje okruh a definici osobních údajů. Osobní údaje jsou jakékoliv informace o identifikované nebo identifikovatelné fyzické osobě. Osobním údajem proto nejsou např. údaje o právnické osobě , nejsou to údaje, které konkrétní osobu neztotožňují. Už směrnice (č. 95/46/ES, předcházející nařízení) naopak mezi osobní údaje zařadila i dynamické IP adresy či jiné virtuální identifikátory.[3] Osobním údajem může být např. i způsob vystupování advokáta v soudním řízení.[4][5]
- Důvodů ke zpracování osobních údajů může být několik. Jinak je se zpracováním osobních údajů třeba vyslovit souhlas. GDPR zakotvuje více titulů ke zpracování osobních údajů, které před tímto souhlasem (případným nesouhlasem) mají přednost.[6] Jedná se například o právní povinnosti, ale i o oprávněný zájem (například marketingové a obchodní zájmy).

POVINNOSTI SPRÁVCŮ

1. **Zpracování údajů**, ať je nařízeno zákonem, prováděno z vůle správce nebo po dohodě či se souhlasem dotčených osob, **musí být legitimní** a nesmí být v rozporu s právními předpisy či morálkou.
2. Každé zpracování údajů musí být **založeno na některém ze základních důvodů** (právních titulů pro zpracování), nejčastěji se jedná o smluvní plnění, výkon právních povinností či plnění zákonného oprávnění, výkon veřejné moci nebo zpracování na základě souhlasu dotčené osoby.
3. Každý, kdo shromažďuje, dále zpracovává a uchovává osobní údaje, musí jasně vymezit (stanovit a být schopen vysvětlit) sledovaný záměr - **účel zpracování údajů**.
4. Všechny způsoby a formy, rozsah zpracování a doba uchovávání údajů musí být **vždy přiměřené účelu zpracování**.
5. Pokud detaily zpracování stanoví veřejnoprávní předpis, nelze se od nich většinou odchýlit. Každé zpracování ve veřejném sektoru musí mít **jasný zákonný podklad**, takové zpracování nelze nahradit souhlasem se zpracováním údajů.
6. Správce i zpracovatel osobních údajů musí osobní údaje **patřičně zabezpečit** a chránit organizačními a technickými opatřeními – v míře odpovídající rizikovosti zpracování.
7. Zpracování by mělo být vůči dotčeným fyzickým osobám prováděno **férově, korektně a transparentně**. Informace o zpracování poskytované subjektu údajů musí být **zřetelné, jednoznačné a srozumitelné, v rozsahu odpovídajícímu konkrétní situaci**.
8. Zpracování **nesmí nadměrně zasahovat do soukromí**. Správci mohou volit různé přiměřené prostředky zpracování, v případě moderních technologií jsou však povinni zvážit nová rizika i dopady do soukromí jednotlivců. Zejména musí uvážit důvodnost a oprávněnost každého sdílení či zveřejnění negativních či jinak citlivých údajů.
9. **Po naplnění účelu zpracování** je dána povinnost osobní údaje **zlikvidovat**. Delší dobu uchování mohou stanovit zákonná pravidla pro archivaci nebo zvláštní využívání údajů (státní statistická služba, nemocenské a důchodové pojištění apod.).
10. V rámci EU je v každé členské zemi zaručena **unifikovaná ochrana osobních údajů**, kterou stanoví obecné nařízení (**GDPR**). Předávat osobní údaje mimo Evropskou unii lze jen za splnění dodatečných pravidel nebo za určitých okolností, jako je např. plnění smlouvy se subjektem údajů.

ZÁVAZNOST

- Nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.
- Nařízení definuje zásady zpracování osobních údajů a podmínky zákonnosti jejich zpracování.
- Upravuje také podmínky vyjádření poskytnutého souhlasu se zpracováním údajů a poskytování informací a přístupu k osobním údajům.

OHLAŠOVACÍ POVINNOST SPRÁVCE VŮČI DOZOROVÉMU ÚŘADU (ČL. 33 GDPR)

- Správce má podle čl. 33 odst. 1 GDPR povinnost ohlásit jakékoliv porušení zabezpečení osobních údajů dozorovému úřadu (v ČR Úřadu pro ochranu osobních údajů), a to bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl (Pokud není ohlášení učiněno do 72 hodin, ale až později, musí být současně s ním uvedeny důvody zpoždění.). Správce tak nemusí učinit, jen pokud je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob (např. v případě používání pseudonymizace či šifrování, které v některých případech mohou riziko pro práva a svobody fyzických osob zcela eliminovat).[10]

Úřad pro ochranu osobních údajů

OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ MUSÍ PODLE ČL. 33 ODST. 3 GDPR PŘINEJMENŠÍM OBSAHOVAT:

- popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů,
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace,
- popis pravděpodobných důsledků porušení zabezpečení osobních údajů,
- popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

GDPR V ČESKU

- upřesňuje Zákon č. 110/2019 Sb., o zpracování osobních údajů. ÚOOÚ dále zmapoval oblasti, kde právní předpisy regulují zpracování osobních údajů podle článku 6 odst. 1 GDPR:[20]
- Elektronická veřejná správa, územní samospráva a doklady
- Fotografie ve veřejnoprávních rejstřících
- Identifikace včetně rodného čísla
- Elektronická komunikace a telekomunikace
- Kamerové systémy
- Veřejnoprávní rejstříky
- Armáda, policie, trestní řízení a zpravodajské služby
- Kromě toho existují sektorové metodiky pro bankovnictví, školství, veřejné zakázky, zdravotnictví a podobně.[21]
- **Spolek pro ochranu osobních údajů**

PRÁVNÍ PŘEDPISY

Ústavní základ ochrany osobních údajů

1. úmluva Rady Evropy č. 108 z roku 1981
2. článek 8 Charty základních práv EU
3. článek 16 Smlouvy o fungování Evropské unie
4. článek 7, 10 odst. 3 a 13 Listiny základních práv a svobod (Ústavní zákon č. 2/1993 Sb. ve znění ústavního zákona č. 162/1998 Sb. a ústavního zákona č. 295/2021 Sb.)

Obecné předpisy ochrany osobních údajů

1. zákon č. 89/2012 Sb., občanský zákoník
2. nařízení Evropského parlamentu a Rady 2016/679 (GDPR)
3. zákon č. 110/2019 Sb., o zpracování osobních údajů

Procesní předpisy

1. zákon č. 500/2004 Sb., správní řád
2. zákon č. 150/2002 Sb., soudní řád správní
3. zákon č. 255/2012 Sb., kontrolní řád
4. zákon č. 99/1963 Sb., občanský soudní řád

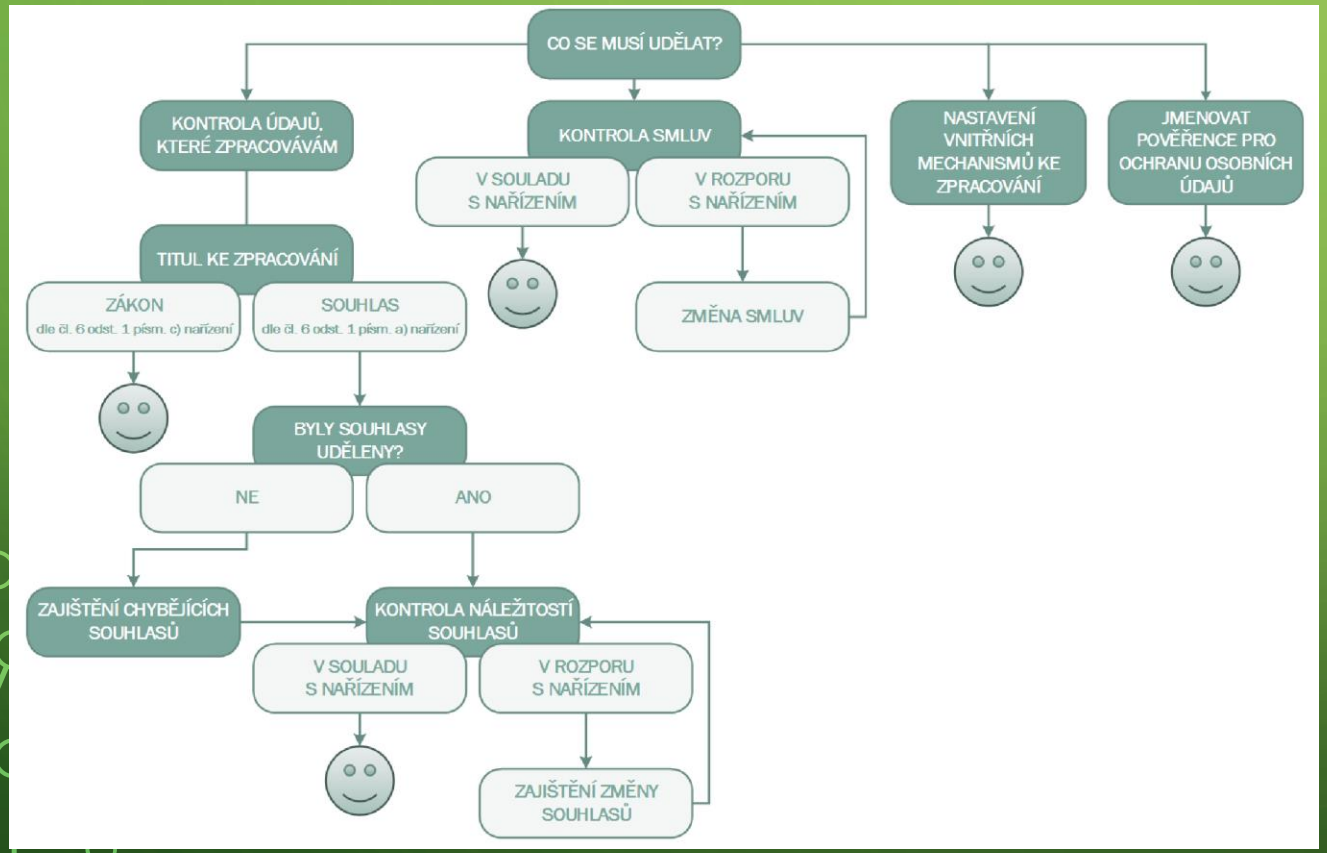
GDPR V MV ČR

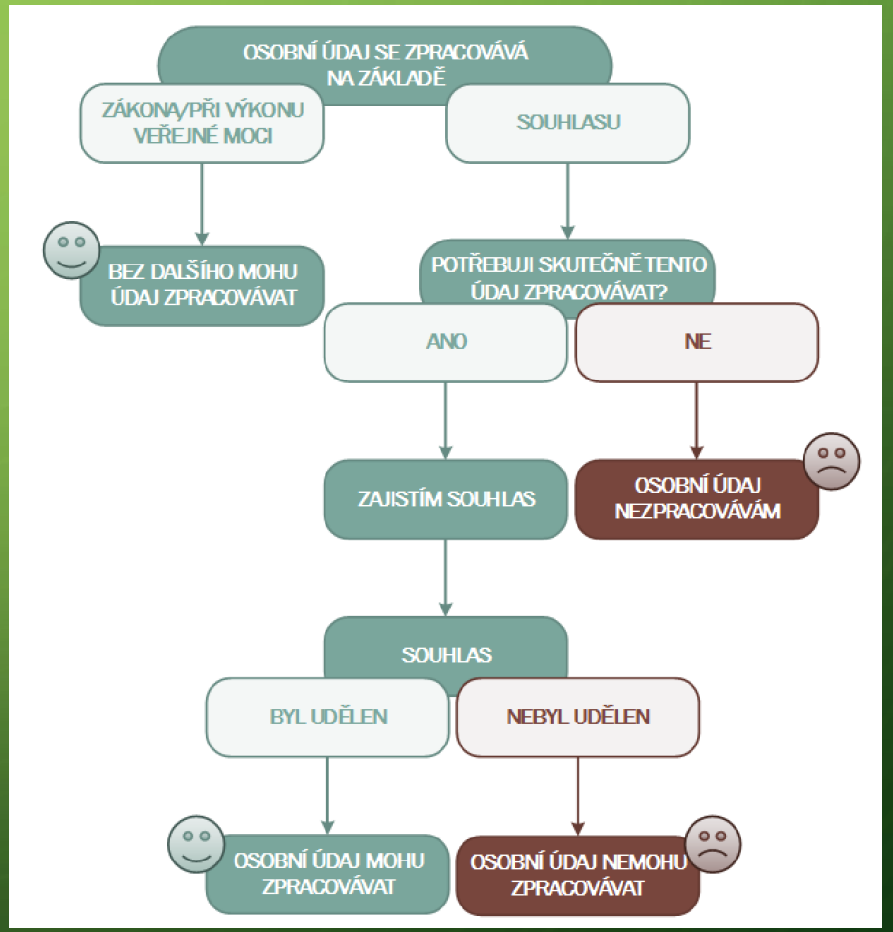
- N A Ř Í Z E N Í Ministerstva vnitra č. 48 ze dne 18. srpna 2006, kterým se upravuje postup při ochraně osobních údajů v Ministerstvu vnitra a v Policii České republiky
- P O K Y N ministra vnitra č. 56 ze dne 13. října 2003, kterým se upravuje zabezpečení ochrany osobních údajů v Ministerstva vnitra a Policii ČR
- N A Ř Í Z E N Í Ministerstva vnitra č. 16 ze dne 4. března 2010, kterým se určuje postup při ochraně osobních údajů evidenčně chráněných osob v informačních systémech celostátních správních evidencí
- N A Ř Í Z E N Í Ministerstva vnitra č. 19 ze dne 15. dubna 2015, kterým se určuje postup při ochraně osobních údajů evidenčně chráněných osob
- P O K Y N ministra vnitra ze dne 7. listopadu 2017, kterým se zřizuje pracovní skupina pro posouzení spisových služeb z hlediska požadavků nařízení GDPR
- P O K Y N ministra vnitra ze dne 7. listopadu 2017, kterým se zřizuje pracovní skupina pro implementaci nařízení GDPR v Ministerstvu vnitra
- **N A Ř Í Z E N Í Ministerstva vnitra č. 34 ze dne 22. října 2018 o postupu při ochraně osobních údajů v Ministerstvu vnitra (změna 31/2021, 31/2022, 16/2023)**
- Nakládání s osobními údaji z pohledu HZS ČR
- Informace o zpracování osobních údajů získaných od zaměstnance/příslušníka – aktualizace (GŘ HZS)
- Informace pro žadatele – právo na přístup k osobním údajům (GŘ HZS)

NEJČASTĚJŠÍ NEDOSTATKY

- chybějící/neaktuální IAŘ, včetně příloh - pověření
- Nedostatečné technicko - organizační opatření k zajištění ochrany zpracovávaných osobních údajů;
- U jednotlivých zpracování stanovit maximální dobu uchování odpovídající účelům zpracování;
- Proškolování pracovníků, kteří jsou pověřeni zpracováním osobních údajů.

CO SE MĚLO UDĚLAT DO DNE NABYTÍ ÚČINNOSTI NAŘÍZENÍ GDPR (25. 5. 2018)





DIGITÁLNÍ AGENDA

- Česká republika má pro digitální regulaci dva základní pilíře: zákon č. 12/2020 Sb., o právu na digitální služby, neformálně „digitální ústava“. Zakotvuje právo na informace ve vztahu k poskytování digitálních služeb a přístupu k osobním údajům.
- Od 1. července 2022 pak zavedl bezvýznamový směrový identifikátor fyzické osoby (BSI) jako náhradu rodného čísla.
- Zákon č. 111/2009 Sb., o základních registrech, zřídil v České republice eGovernment jako mechanismus pro sdílení dat uvnitř veřejného sektoru.

DIGITÁLNÍ AGENDA

1. V působnosti Ministerstva průmyslu a obchodu je **akt o správě dat** (angl. European Data Governance Act, **DGA**) vydaný pod číslem 2022/868, platný od 3. června 2022. Jeho cílem je usnadnit sdílení dat veřejného sektoru.
2. V působnosti Úřadu pro ochranu hospodářské soutěže je **akt o digitálních trzích** (angl. Digital Markets Act, **DMA**) vydaný pod číslem 2022/1925, platný od 12. října 2022. Jeho cílem je nastavení pravidel pro přístup ke konkrétní oblasti digitálního trhu.
3. V působnosti Ministerstva průmyslu a obchodu je **akt o digitálních službách** (angl. Digital Services Act, **DSA**) vydaný pod číslem 2022/2065, platný od 27. října 2022. Je novou regulací elektronického obchodu.
4. V působnosti Ministerstva průmyslu a obchodu je **návrh aktu o datech** (angl. Data Act, **DA**. Jeho cílem je usnadnit sdílení dat soukromého sektoru, zejména pomocí interoperability jednotlivých zařízení.
5. V působnosti Úřadu vlády je **návrh aktu o umělé inteligenci** (angl. Artifical Intelligence Act, **AIA**), který se má zabývat potenciálně nebezpečnými technologiemi.
6. **V působnosti Ministerstva vnitra je návrh nařízení o evropské digitální identitě (angl. European Identity Digital Regulation, EIDR), neformálně o „digitální peněžence“, což je rozšíření nařízení o službách vytvářejících důvěru (angl. Electronic Identification, Authentication and Trust Services, eIDAS), na soukromý sektor.**
7. V působnosti Ministerstva průmyslu a obchodu je **návrh nařízení o soukromí a elektronických komunikacích** (angl. ePrivacy Regulation, **ePR**), který má zajistit důvěrnost elektronických komunikací a který je projednáván již od roku 2017.

ELEKTRONIZACE PROCESŮ

- **Zákon č. 300/2008 Sb.**, o elektronických úkonech a autorizované konverzi dokumentů
- **Zákon č. 499/2004 Sb.**, o archivnictví a spisové službě a o změně některých zákonů
- **Vyhláška č. 96/2023 Sb.** ze dne 31. března 2023 kterou se mění vyhláška č. 259/2012 Sb. o podrobnostech výkonu spisové služby ve znění pozdějších předpisů
- **Oznámení Ministerstva vnitra,** kterým se zveřejňuje národní standard pro elektronické systémy spisové služby VMV čá. 42/2023. Znění účinné od 1. července 2023

REFERENCE

1. NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 pdf, html
2. ŠALAMON, Tomáš. Připravte se na GDPR - Osobní údaje jsou všude. *Incomaker* [online]. 9. listopadu 2017. Dostupné v archivu pořízeném dne 2017-12-22.
3. NEŠPŮREK, Robert. Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj. *Právní prostor* [online]. 24. května 2017. Dostupné online.
4. LOBOTKA, Andrej. Způsob vystupování advokáta v soudním řízení je osobním údajem. *SMART LAW* [online]. 2019-02-08 [cit. 2020-03-06]. Dostupné v archivu pořízeném z originálu dne 2020-07-10.
5. Rozsudek Krajského soudu v Brně ze dne 7. 11. 2018, č. j. 31 A 68/2018–177.
6. https://www.businessinfo.cz/navody/souhlas-se-zpracovanim-osobnich-udaju-kdy-ho-potrebujete/ - Souhlas se zpracováním osobních údajů: Kdy ho potřebujete?
7. https://echo24.cz/a/S9u4h/prvni-den-gdpr-facebook-a-google-celi-zalobe-za-200-miliard - První den GDPR: Facebook a Google čelí žalobě za 200 miliard
8. https://phys.org/news/2018-06-facebook-google-users-eu-law.html - Facebook, Google 'manipulate' users to share data despite EU law: study
9. https://techxplore.com/news/2023-03-websites-comply-privacy-laws-track.html - The most visited websites do not comply correctly with privacy laws and actively track their users, finds Spanish study

10. LOBOTKA, Andrej. Ohlašování porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů. *SMART LAW* [online]. 2020-02-17 [cit. 2020-03-05]. Dostupné v archivu pořízeném z originálu dne 2020-07-10.
11. Formulář ohlášení porušení zabezpečení osobních údajů dle GDPR.. *www.uoou.cz* [online]. [cit. 2020-03-05]. Dostupné v archivu pořízeném z originálu dne 2020-07-10.
12. LOBOTKA, Andrej. Povinnost oznámit porušení zabezpečení osobních údajů subjektům údajů. *SMART LAW* [online]. 2020-02-24 [cit. 2020-03-06]. Dostupné v archivu pořízeném z originálu dne 2020-07-10.
13. ČTK. GDPR se dotkne i živnostníků. Drtivá většina o tom neví. *Týden.cz* [online]. 24.11.2017 19:40. Dostupné online.
14. -jan-. Školy se s obavami připravují na novou směrnici EU. *Týden.cz* [online]. 21.03.2018 20:54. Dostupné online.
15. GDPR stručně: Úřad pro ochranu osobních údajů. *www.uoou.cz* [online]. [cit. 2018-08-31]. Dostupné online.
16. Souhlas se zpracováním údajů by měly děti smět dát od 15 let. *Týden.cz* [online]. 21.03.2018 09:18. Dostupné online.
17. CECHL, Pavel; BAROCH, Pavel. Nový příkaz z Bruselu: strážce dat v každé vsi. *Týden.cz* [online]. 22.09.2017 12:55. Dostupné online.
18. Zákon o zpracování osobních údajů
19. ÚOOÚ. *ÚOOÚ nemohl udělit pokutu ministerstvu, neumožňuje mu to zákon* [online]. Rev. 9.8.2019 [cit. 2019-09-03]. Dostupné v archivu pořízeném dne 2019-09-03.
20. ÚOOÚ: Průřezové oblasti zpracování osobních údajů
21. Metodiky vybraných institucí k sektorovým zpracováním osobních údajů