STRUČNÝ PRŮVODCE GDPR správou

Jak na GDPR?

FLACO Group s.r.o., Juliánovské nám. 2, 636 00 Brno
www.flacogroup.cz

V Brně 2018

obchod@flacogroup.cz

Obsah

Úvod

Dnem 25. května 2018 nabývá účinnosti nařízení Evropské unie o ochraně osobních dat, tzv. GDPR (General Data Protection Regulation).

Dnes se potkáváme se zprávy, které obsahují alespoň některá z uvedených informací:

* Vztahuje se úplně na všechny bez ohledu na to, zda jde o podnikatele či nikoliv, a bez ohledu na velikost, tzn. nedělá rozdíly, zda jste OSVČ, malá firma nebo korporátní organizace.
* Veškeré informace, které nařízení stanovuje, jsou definovány neurčitě a mlhavě.
* Kroky k naplnění povinností stanovených dotčeným nařízením jsou časově a finančně náročné.
* Za porušení hrozí mnohamilionové pokuty, které mohou být likvidační pro vaše podnikání. (20 miliónů EUR nebo 4 % z celosvětového obratu celé skupiny podniků, a to podle toho, která částka bude vyšší!)

Víte, co je na těchto tvrzeních pravdivé? **Úplně všechno!**

V současnosti je spousta subjektů, zejména malých podnikatelů, kteří si myslí, že se jich nařízení netýká, případně, že se jim moc nestane, když jej budou ignorovat. Nedejte se mýlit – toto nařízení se dotkne úplně každého, a proto jej ignorovat, může znamenat i konec vašeho podnikání zásluhou pokut.

Většina dnes dostupných materiálů a poradenských firem v oblasti ochrany osobních údajů se soustřeďuje na velké společnosti, nadnárodní korporace nebo státní správu, kterým může nabídnout drahá a komplikovaná řešení. Proto jsme si dovolili připravit tohoto stručného průvodce, který může sloužit všem bez rozdílů velikostí.

Tento **Stručný průvodce GDPR správou** Vám nenabídne lásku, partnera, jak být úspěšný, peníze nebo oblibu, na to je tu spousta jiných aktivit, ale rozhodně Vám **pomůže ušetřit peníze a čas**, který byste věnovali hledáním informací na vlastní pěst.

Všechny informace, které budou uvedeny v našem Stručném průvodci GDPR správou, jsou informativní a jakékoliv použití informací z něj je tak pouze ve vašich rukou a společnost FLACO Group s.r.o. nenese žádnou odpovědnost. Tyto informace mají pouze doporučující charakter, a to i z důvodu, že každá firma je jedinečná, stejně jako samotný člověk a nedá se napsat přesný postup, který je aplikovatelný pro všechny.

V každé kapitole se vynasnažíme napsat i to, co je potřeba si odnést do praxe.

Co to vlastně je GDPR?

GDPR (správně čti dží-dý-pí-ár), je zkratka pro General Data Protection Regulation, česky to znamená Obecné nařízení o ochraně osobních údajů.

Toto nařízení představuje dosud nejucelenější soubor pravidel na ochranu osobních údajů fyzických osob nikoli pouze v evropském, ale i celosvětovém měřítku. GDPR je přímo aplikovatelné nařízení Evropské unie, což znamená, že jednotlivé členské země Evropské unie toto nařízení netransformují do svých právních řádů ve formě samotně vydaných zákonů, ale přímo ho používají ve znění, jak ho vydala Evropská unie bez možnosti úpravy.

V minulosti byla ochrana osobních údajů ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů na vnitrostátní úrovni známým zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých údajů.

Účelem Obecného nařízení o ochraně osobních údajů je tedy sjednocení pravidel zacházení s osobními údaji v celém prostoru Evropské unie a pro všechny občany států bez ohledu na jejich umístění ve světě.

Obecné nařízení tak sebou přináší:

* Rovnocennou vymahatelnost práv v oblasti ochrany osobních údajů
* Stejné sankce
* Těsnější spolupráci dozorových orgánů

GDPR začíná v celé Evropské unii jednotně platit od
25. května 2018.

Základní pojmy a pravidla

V následující části si projdeme základní pojmy z GDPR a některá pravidla a povinnosti při zpracování osobních údajů a práva dotčených osob.

Místní působnost

Ačkoliv je GDPR předpisem Evropskou unií, dopadá i na subjekty sídlící mimo EU. Je tomu tak v i případě, kdy správce nebo zpracovatel údajů sice sídlí mimo EU, ale na území EU zřídí pobočku (pozn. Pobočko use rozumí i jeden obchodní zástupce, který disponuje právní identitou – IČO a počítačem, ze kterého vyřizuje objednávky), jejíž činnost se zpracováním údajů souvisí.

Co si odnést do praxe:

* Nabízení služeb v zahraničí nebo skutečnost, že organizace má mateřskou společnost v jiném členském státu EU, může znamenat, že pověřenec (DPO) nebo osoba, která má na starosti danou problematiku ve společnosti, bude muset komunikovat se zahraničním dozorovým orgánem.
* Odpovědná osoba nebo pověřenec musí vědět, kterých dalších států se přeshraniční prvek týká, a které dozorové orgány se na něj mohou obrátit. Musí mít také představu na koho se obrátit o spolupráci (jazyková bariéra nebo nutnost aplikovat část zahraniční právní úpravy.

Subjekt údajů

Subjektem údajů se rozumí jakákoli identifikovaná a identifikovatelná fyzická osoba (občan), jejíž totožnost je přímo zřetelná, nebo kterou lze přímo či nepřímo identifikovat zejména s odkazem na určitý identifikátor nebo na jeden i více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této osoby.

Co si odnést do praxe:

* Typicky půjde o fyzickou osobu identifikovanou jejím Jménem a Příjmením.

Osobní údaj

Osobním údajem je každá informace, která se týká přímo nebo nepřímo určené nebo určitelné fyzické osoby (čl. 4 písmeno a) GDPR).

Co si odnést do praxe:

* GDPR se nevztahuje na informace o právnických osobách (název, činnost, majetek apod.), ale na druhé straně se do určité míry vztahuje i na fyzické osoby podnikající.

Dále pak na členy orgánů právnických osob a samozřejmě na zaměstnance soukromých subjektů i orgánů státní správy a samosprávy.

* GDPR se vztahuje pouze na živé osoby nikoliv na mrtvé.
* Osobním údajem je prakticky cokoliv (jméno, příjmení, adresu, datum narození, email, telefon, korespondenční adresa, nákupy, platební morálka, účet v bance. U zaměstnanců pak se to rozšiřuje o průběh pracovněprávního vztahu, kvalifikace, plat, vyživované osoby, docházka a mnoho dalšího.

Poučka: Pokud správce údajů vede evidenci osob, respektive databázi informací, které sice nedokáže sám s konkrétní osobou spojit, ale má legální a technickou možnost, jak tyto informace propojit s konkrétní osobou, pak se rovněž jedná o osobní údaj.

Příkladem může být organizace, která provozuje kamerový systém na veřejném prostranství. Organizace sice nedokáže identifikovat osobu, ale pokud záznam předá policii, a ta může pro identifikaci využít další zdroje informací, tak se jedná o její osobní údaje (té dotyčné osoby). Organizace má legální možnost jak nepřímo (prostřednictvím policie) identifikovat dotyčnou osobu. Jedná se tak o sběr osobních údajů.

Citlivé osobní údaje

Kromě běžných osobních údajů GDPR vymezuje pojem i tzv. citlivé osobní údaje neboli zvláštní kategorie údajů (č. 9 odstavce 1 GDPR). Mezi takové údaje se řadí:

* Údaje o rasovém či etnickém původu.
* Údaje o politických názorech, náboženství nebo filosofickém přesvědčení.
* Informace o členství v odborech.
* Údaje o zdravotním stavu (např. pedikúra – diabetes).
* Údaje o sexuálním životě nebo sexuální orientaci.
* Genetické údaje, údaje vypovídající o genetickém vybavení konkrétního člověka.
* Biometrické údaje zpracované za účelem identifikace člověka (např. otisk prstu u docházkového systému).
* Údaje týkající se rozsudků v trestních věcech a spáchaných trestných činů (čl. 10 GDPR).

Rodné číslo

Rodné číslo tvoří samostatný a specifický údaj. Nejedná se o citlivý, protože není uvedeno mezi kategoriemi výše, ale na druhé straně jej nelze označit za běžný osobní údaj, protože možnost a předpoklady pro jeho využití jsou upraveny ve zvláštním předpisu, který má při zpracování rodného čísla přednost (Zákon č. 133/2000 Sb. O evidenci obyvatel a o rodných číslech, zejména v § 13c).

Rodné číslo lze využívat, zpracovávat, pouze tehdy, pokud správce:

* Je orgánem státní správy, soudem nebo notářem a jedná v rámci svých veřejnoprávních kompetencí.
* Je mu to uloženo nebo výslovně umožněno zvláštním zákonem (např. pojišťovnictví).
* Získá souhlas nositele rodného čísla.

Zpracování údajů

Zpracováním se rozumí jakákoliv operace nebo soubor operací s osobními údaji, kterou správce systematicky a za jasným účelem provádí. Jedná se o shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění údajů, jejich vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv další zpřístupnění, seřazení či kombinování, omezení, výmaz nebo zničení. Celé tyto procesy mohou být za použití automatizovaných postupů nebo bez něj.

Co si odnést do praxe:

* O zpracování osobních údajů v režimu GDPR se jedná vždy pokud je zpracování prováděno automatizovanými prostředky (např. schválení půjček za pomocí nahlédnutí do registru dlužníků na základě algoritmu).
* Zejména v prostředí internetu či obecně při zpracování dat za využití prostředků informačních a komunikačních technologií, je nutno pojem zpracování osobních údajů vykládat široce.
* V případě čistě manuálního zpracování informací a dokumentů, které mohou obsahovat osobní údaje, je pro posouzení, zda se na danou činnost bude vztahovat GDPR, podstatné, zda osobní údaje jsou nebo alespoň mají být zařazovány do databáze či evidence, ve které lze údaje vyhledávat či třídit podle předem určených kritérií (např. filtr v excelu).
* Zpracováním údajů v režimu GDPR je i jednorázová a časově omezená operace (např. pouhé zveřejnění nebo poskytnutí údajů o několika málo osobách dalšímu jedinci)

Správce

Správcem osobních údajů je každý subjekt bez ohledu na právní formu – tzn. Vy sami, který se rozhodne o tom, že bude osobní údaje zpracovávat, jinak řečeno stanoví účel a prostředky zpracování.

E-shop se rozhodne, že bude nabízet výrobky či služby spotřebitelům a v souvislosti s objednávkou a dodáním zboží musí zpracovávat osobní údaje. Subjekt v jakémkoliv postavení se může rozhodnout, že bude svůj majetek či pozemky chránit kamerovým systémem. Každý zaměstnavatel je správcem údajů svých zaměstnanců apod.

Odpovědnost správce – je jedním z nových pravidel GDPR a přináší princip odpovědnosti, či spíše doložitelné odpovědnosti za soulad zpracování osobních údajů s právem. (tzn. tento soulad průběžně monitorovat a hodnotit) a nelze to dělat zpětně! Správce musí vždy doložit, že zpracování již od počátku bylo koncipováno jako zákonné a že tak bylo i nastaveno. Dále že jeho praktická realizace je monitorována a že jsou nastaveny i další procesy a kontrolní mechanismy, aby zpracování probíhalo tak jak má.

Nástroji pro toto doložení jsou:

* Záznamy o činnostech zpracování
* Koncept záměrné a standardní ochrany osobních údajů (např. Směrnice pro nakládání s osobními údaji)

* Povinnost správce posuzovat a ověřovat zpracovatele osobních údajů (náležitosti zpracovatelské smlouvy).
* Pravidla pro ohlašování případů porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a v některých případech i dotčeným osobám (např. Směrnice pro nakládání s osobními údaji).
* Pověřenec pro ochranu osobních údajů.
* Kodexy a certifikáty.

Zpracovatel

Zpracovatelem osobních údajů je subjekt, který provádí zpracování údajů pro správce. Správce stanoví účel a zpracovatel část nebo celé zpracování provádí místo správce. V případě Zpracovatele se vždy jedná o subjekt s vlastní právní subjektivitou (např. IČO), o dodavatele (např. účetní firma).

Typickým zpracovatelem je:

* Poskytovatel cloudových služeb, které správce využívá pro zpracování osobních údajů.
* Bezpečnostní agentura využívající kamerový systém.
* Externí mzdová účetní
* Externí archiv.
* Společnost provádějící likvidaci nosičů osobních údajů.
* Agentura shromažďující a připravující osobní údaje pro přímý marketing.

Co si odnést do praxe:

* Organizace může být pro různá zpracování správcem nebo zpracovatelem osobních údajů zároveň.
* Organizace by měla evidovat všechny agendy, při kterých dochází při zpracování osobních údajů ke spolupráci s dalšími subjekty a odlišovat, ve kterých je správcem a kdy je zpracovatelem.
* Pokud u správce nebo zpracovatele působí pověřenec pro ochranu osobních údajů (DPO), součást jeho agendy může být právě posuzování a evidování správcovsko – zpracovatelských vztahů.

Základní zásady zpracování osobních údajů:

* Zákonnost zpracování (čl. 6–10 GDPR)
* Transparentnost zpracování (čl. 13 a 14 GDPR)
* Účelové omezení (čl. 40 GDPR)
* Minimalizace údajů (čl. 5 odstavec 1 písmeno c) GDPR)
* Přesnost údajů
* Omezení uložení údajů (čl. 5 odstavec 1 písmeno e) GDPR)
* Bezpečnost a integrita dat (§ 629 odstavec 1 zákona č. 89/2012 Sb., občanský zákoník)
* Doložitelná odpovědnost za soulad GDPR

Souhlas

Souhlasem subjektu údajů se rozumí jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášení či jiným zjevným potvrzením své povolení ke zpracování svých osobních údajů. A to včetně informace, jak tento souhlas odvolat.

Dozorový úřad

V podmínkách České republiky je dozorovým úřadem Úřad pro ochranu osobních údajů (www.uoou.cz), nadřízený mu pak je Evropský sbor pro ochranu osobních údajů.

Práva dotčených osob

GDPR upravuje řadu práv osob, jejichž údaje jsou zpracovávány. Smyslem je posílit kontrolu subjektů údajů nad zpracováním jako takovým a zvýšit jeho transparentnost.

Jde především o tato práva dotčených osob:

* Právo na informace o zpracování včetně přístupu ke kopii zpracovávaných údajů.
* Právo na opravu zpracovávaných údajů.
* Právo na výmaz osobních údajů.
* Právo na omezení zpracování.
* Právo na přenositelnost údajů.
* Právo na námitku.
* Právo napadnout automatizované rozhodnutí.

Společná pravidla pro výkon práv

Pro zajištění práv dotčených osob GDPR zavádí několik společných pravidel a postupů, které je správce povinen respektovat, ať už u něj subjekt údajů uplatní kterékoliv ze svých práv.

1. Správce by měl výkon práv subjektu údajů usnadňovat.
2. Správce by měl zajistit podmínky pro to, aby žádosti mohli být podávány elektronicky, zejména v případě zpracování osobních údajů elektronickými prostředky. Na druhou stranu je však správce povinen dostatečná opatření, aby subjekt údajů jasně a jednoznačně identifikoval.
3. Správce je povinen subjekt údajů informoval o tom, jak byl jeho podnět vyřízen, a to obvykle do 30 kalendářních dní od jeho obdržení. (lhůtu lze prodloužit o další 2 měsíce v případě složitosti případů či počtem žádostí, ale je povinen o tom subjekt údajů informovat).
4. Pokud správce jmenuje Pověřence pro ochranu osobních údajů je povinen zveřejnit jeho kontaktní údaje.

Co si odnést do praxe:

* Aby byl správce schopen doložit, že plní či je připraven plnit své povinnosti i při výkonu práv subjektů údajů, měl by mít nastavený a zdokumentovaný proces pro příjem, vyřizování a evidování těchto podnětů včetně určení odpovědnosti jednotlivých zaměstnanců či oddělení/útvarů/sekcí.
* Správce by měl výkon práv subjektům údajů usnadňovat, avšak s ohledem na charakter své činnosti a standardně používané komunikační kanály.
* Správce je povinen ověřit identitu subjektu, který konkrétní žádost podal, aby nedošlo k neoprávněnému zásahu do práv jiné osoby.
* Pověřenec pro ochranu osobních údajů nebo kdokoliv, kdo je v organizaci odpovědný za soulad zpracování osobních údajů s GDPR, by měl mít možnost posoudit způsob vyřízení konkrétních žádostí.

Právo na informace

Prvním z práv subjektů údajů ke toto právo na informace a zpracování osobních údajů včetně práva na přístup ke kopii zpracovávaných údajů.

Jaké jsou náležitosti, pokud identifikuje subjekt údajů?

1. Sdělit, zda informace zpracovává či nikoliv.
   V případě, že ano tak následuje:
2. Účely zpracování údajů
3. Kategorie údajů (identifikační, popisné, kontaktní atd.)
4. Jací jsou příjemci údajů nebo jakým kategorií příjemců byly nebo budou či mohou být osobní data subjektu údajů zpřístupněny.
5. Plánovaná doba, po kterou budou jeho údaje zpracovávány.
6. Existenci práva subjektu údajů požadovat od správce opravu nebo výmaz osobních údajů, omezení jejich zpracování, práv vznést námitku proti tomuto zpracování a právo podat stížnost u dozorového orgánu.
7. Veškeré dostupné informace o zdrojích osobních údajů, pokud nejsou získány od subjektu údajů.
8. Skutečnost, že dochází k automatizovanému rozhodování, které má právní nebo obdobné účinky na subjekt údajů a smysluplné informace týkající se použitého postupu, významu a předpokládaných důsledků takového zpracování.
9. Pokud jsou osobní údaje subjektu údajů předávány do třetí země mimo EU, má subjekt údajů právo být informován o vhodných zárukách pro ochranu jeho dat.

Právo na opravu

Právo na opravu koresponduje s povinností správce zpracovávat pouze přesné a aktuální údaje.

Co si odnést do praxe:

* Pokud se správce od subjektu údajů dozví, že jím aktivně zpracovávané údaje jsou nepřesné či neaktuální, musí je opravit ve všech relevantních databázích či evidencích.
* Pro splnění této povinnosti je vhodné nastavit a zdokumentovat proces popisující, jak správce bude postupovat, a to od přijetí žádosti, přes její posouzení až po vyřízení a zajištění toho, že zpracovávané údaje budou všude aktualizovány.

Právo na výmaz („Právo být zapomenut“)

GDPR upravuje i právo na výmaz osobních údajů. Je zde ale potřeba zdůraznit, že se v zásadě o nové pravidlo nejedná.

Správce je povinen osobní údaje konkrétního člověka vymazat, pokud:

* Osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány. Tato povinnost odpovídá zásadě omezení uložení, podle které nelze údaje uchovávat déle, než je nezbytně nutné pro dosažení účelu zpracování.
* Subjekt údajů odvolá souhlas se zpracováním a správce údajů nemá žádný další právní důvod pro jejich zpracování.
* Subjekt údajů vznese námitku proti zpracování prováděném na základě oprávněného zájmu a správce po přezkoumání dospěje k tomu, že práva dotčen osoby v daném případě nad jeho oprávněným zájmem skutečně převažují.
* Pokud správce údaje zpracovává pouze za účelem adresného marketingu, je povinen jen bez dalšího vymazat, pokud proti tomu subjekt údajů vznese námitku.
* Správce je povinen údaje vymazat, pokud byly zpracovávány protiprávně, nebo je výmaz správci uložen právem.
* Jestliže byly osobní údaje shromážděny při nabízení služeb informační společnosti osobě mladší 18 let s jejím souhlasem, je správce povinen tyto údaje vymazat na základě prosté žádosti dotčené osoby.

Co si odnést do praxe:

* Právo na výmaz osobních údajů není absolutní, lze jej uplatnit jen v omezeném okruhu případů, a i pak existují výjimky, kdy správce není povinen osobní údaje vymazat.
* Pokud je další zpracování údajů v okamžiku uplatnění práva na výmaz nezbytné pro plnění právní povinnosti správce, pro plnění smlouvy se subjektem údajů (např. záruční doba) nebo pro oprávněný zájem správce či další osoby, právo na výmaz se neuplatní.
* Rovněž pro realizaci práva na výmaz je vhodné nastavit a zdokumentovat celý proces.
* V případě, kdy je správce povinen údaje vymazat, musí tak učinit ze všech dotčených systémech a databázích. Pokud údaje zveřejnil, je povinen vynaložit přiměřené a odůvodněné úsilí k tomu, aby o výmazu údajů informoval i příjemce.

Právo na omezení zpracování

Toto právo se zakládá na č. 18 GDPR a spočívá v tom, že správce dané údaje nevymaže, ale jejich aktivní využití (např. pro marketing) dočasně zastaví.

Dotčená osoba může právo na omezení zpracování uplatnit v zásadě pouze ve třech případech:

1. Dotčená osoba se zpracováním svých osobních údajů nesouhlasí, že namítá jejich nepřesnost
2. Dotčená osoba se zpracování svých osobních údajů nesouhlasí, protože uplatnila námitku proti zpracování a tvrdí, že její práva převažují oprávněný zájem správce.

3. Dotčená osoba naopak další uchování údajů požaduje pro ochranu svých práv, byť by správce sám jinak byl povinen údaje smazat (např. pro řešení soudních sporů).

Co si odnést do praxe:

* Forma omezení údajů musí být přizpůsobena konkrétním podmínkám a prostředkům zpracování údajů správce.
* Správce by měl i ve vlastním zájmu námitky vyřídit co nejrychleji, aby mohl údaje i nadále v plném rozsahu zpracovávat.
* Pokud správce námitku vyřídí a subjekt údajů ji v nezměněné formě vznese znovu, správce již není povinen ji detailně zkoumat a zpracování údajů znovu omezovat.

Právo na přenositelnost

Toto právo je zcela novým právem subjektu údajů, které GDPR přináší. Obsahem tohoto práva je povinnost správce, aby osobní údaje, které o subjektu údajů zpracovává s jeho souhlasem nebo v rámci plnění smlouvy, na základě žádosti poskytl subjektu nebo jinému správci, kterého subjekt údajů označí, a to ve strukturovaném, běžně používaném a strojově čitelném formátu.

Co si odnést do praxe:

* Právo na přenositelnost se netýká všech osobních údajů, které správce zpracovává. Dopadá pouze na automatizovaně zpracovávané údaje, a to tehdy, pokud je správce zpracovává na základě souhlasu nebo v rámci plnění smlouvy se subjektem údajů.
* Správce musí být připraven osobní údaje subjektu či jinému příjemci předat ve strukturovaném a strojově čitelném (otevřeném) formátu. Proto je vhodné být na tuto variantu již dopředu připraven a mít zvolený postup a formát, jakým správce bude tuto žádost vyřizovat a údaje předávat.

Právo na námitku

Zpracovává-li správce osobní údaje na základě právního důvodu oprávněného zájmu nebo při výkonu úkolu ve veřejném zájmu, může subjekt údajů proti takovému zpracování uplatnit námitku spočívající v jeho konkrétní situaci. Subjekt údajů tak obecně nezpochybňuje existenci daného právního titulu, ale dokládá, že v jeho konkrétním případě a s ohledem na jeho specifikovanou situaci by zpracování nadále nemělo být prováděno.

Co si odnést do praxe:

* Správce je povinen subjekt údajů o tomto právu výslovně informovat odděleně od dalších informací tak, aby bylo zajištěno, že si subjekt údajů tohoto svého práva bude vědom.
* Vyřízení námitky bude obvykle vyžadovat detailní posouzení celé věci, nové provedení balančního testu a právní argumentaci. Lze proto doporučit využití interních nebo externích právních zdrojů.

Právo na přezkum automatizovaného rozhodnutí

Pokud správce provádí automatizovanými prostředky zpracování osobních údajů, které má pro subjekt údajů právní nebo obdobně významné důsledky, např. při posuzování žádosti o uzavření smlouvy o úvěru nebo pojistné smlouvy, může subjekt údajů správce požádat o přezkum tohoto rozhodnutí.

Co si odnést do praxe:

* Správce není povinen na základě žádosti o přezkumu či vyjádření subjektu údajů své původní rozhodnutí automaticky přehodnotit (např. poskytnout původně odmítnutý úvěr). Daný případ, ale musí být znovu posouzen a to člověkem.
* Správce, respektive jeho zaměstnanci, nemusejí manuálně procházet veškerá kritéria, která byla posuzována, ale postačí kontrola toho, zda algoritmus fungoval správně či posouzení kritérií, na jejichž základě (např. K.O. kritéria) nebyla smlouva uzavřena.

Nové povinnosti pro dokládání souladu s GDPR

GDPR přináší řadu nových procesních a administrativních povinností, které jsou správci a zpracovatelé osobních údajů povinni plnit, aby zajistili a byli i zpětně schopni doložit soulad svojí činnosti s právním rámcem pro zpracování osobních údajů.

Zabezpečení zpracování

Každý správce osobních údajů, teda i Vy, je povinen s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku. Totéž se vztahuje i na zpracovatele osobních údajů.

Pro zabezpečení zpracování se musí brát v potaz všechny související okolnosti a rizika, zohledňují se i náklady.

Je to pochopitelné, malá organizace nebo OSVČ nedokáže investovat řekněme do několika stovek klientů stejné prostředky jako velké organizace nebo státní správa operující s rozpočty v řádech miliónů a osobními údaji tisíců i více fyzických osob.

Záznamy o činnostech zpracování

Správci i zpracovatelé osobních údajů jsou povinni dokumentovat podle čl. 30 GDPR, jaká zpracování osobních údajů provádí, za jakým účelem, a jaké jsou některé další parametry zpracování.

GDPR ukládá, aby správci i zpracovatelé tuto povinnost plnili formou **písemně** vedených záznamů o činnostech zpracování. Ty mají sloužit nejen správci a zpracovateli k tomu, aby měl přehled o své činnosti, ale správce a zpracovatel je povinen záznamy kdykoliv na vyžádání předložit dozorovému úřadu, který je může využít pro monitorování souladu činnosti dané organizaci s GDPR.

GDPR vysloveně vypočítává, jako informace musí vést v záznamech správce a jaké zpracovatel osobních údajů.

U Správce se jedná:

* Jméno (identifikaci) a kontaktní údaje správce a jméno a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl u správce jmenován.
* Účely zpracování. Typickými účely zpracování tak bude např. shromažďování osobních údajů pro účely marketingu, uzavírání a plnění smluv s klienty, ověřování klientů, ale i ochrana majetku (kamery), personální agenda, mzdová agenda apod.
* Ke každému účelu zpracování je správce povinen uvést kategorii dotčených osob (klienti, bývalí klienti, zaměstnanci atd.) a kategorii zpracovávaných údajů (identifikační údaje, kontaktní, popisné atd.).
* Kategorie příjemců, kterým budou nebo mohou být osobní údaje předávány. Typicky půjde o další členy podnikatelské skupiny, orgány státní správy a dále zpracovatele podílející se na některých částech zpracování.
* Informace o předání osobních údajů do třetí země, její určení a označení záruk pro ochranu osobních údajů v některých specifických situacích (standardní smluvní doložky, závazná podniková pravidla apod.).
* Je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií osobních údajů.
* Je-li to možné, obecný popis technických a organizačních bezpečnostních opatření přijatých k ochraně zpracovávaných osobních údajů.

U Zpracovatele se jedná:

* Jméno (identifikaci) a kontaktní údaje zpracovatele a jméno a kontaktní údaje pověřence pro ochranu osobních údajů, pokud byl u zpracovatele jmenován.
* Identifikace správce, pro kterého zpracovatel osobní údaje zpracovává.
* U každého správce potom kategorii (druh) zpracování, které pro něj zpracovatel provádí.
* Informace o předání osobních údajů do třetí země, její určení a označení záruk pro ochranu osobních údajů v některých specifických situacích (standardní smluvní doložky, závazná podniková pravidla apod.).
* Je-li to možné, obecný popis technických a organizačních bezpečnostních opatření přijatých k ochraně zpracovávaných osobních údajů.

Záznamy musí být vedeny písemně, aby mohly být kdykoliv předloženy dozorovému orgánu. Písemnou formou se rozumí i elektronické vedení záznamů, ať už v některém z obecných nástrojů (textový editor, tabulkový editor), nebo jako samostatné aplikace na správu a udržování záznamů o zpracování.

Kdy se povinnost vést Záznamy o činnostech zpracování nemusí vést?

Povinnost vést Záznamy o zpracování se nevztahuje na správce a zpracovatele, kteří mají **méně než 250 zaměstnanců a zároveň**:

* Neprovádějí zpracování, které může představovat riziko pro práva dotčených osob; riziko může být spatřováno např. ve větším rozsahu zpracovávaných údajů (profilování, dlouhodobé sledování dotčené osoby) či účelu zpracování (přiznávání práv či povinnosti, uzavření smluv atd.).
* Jimi prováděné zpracování osobních údajů není pouze příležitostné; pokud je zpracování osobních údajů nezbytné pro hlavní předmět činnosti správce (např. poskytování či zprostředkování nebankovních úvěrů nebo pojištění fyzickým osobám, monitorování veřejně přístupných prostor – kamery, poskytování cloudových služeb pro poskytování osobních údajů).
* Nezpracovávají citlivé osobní údaje. (pedikéři – zdravotní stav zákazníků diabetes, apod.)

Co si odnést do praxe:

* Záznamy o činnostech zpracování jsou povinni vést všichni správci a zpracovatelé, kteří mají více než 250 zaměstnanců a zároveň ti (i když mají mně zaměstnanců) pokud provádějí zpracování představující významné riziko pro dotčené osoby, pravidelné a systematické zpracování osobních údajů či zpracovávají citlivé údaje.
* I pokud na správce či zpracovatele nedopadá vést záznamy o činnostech zpracování, lze doporučit, aby měl alespoň základní přehled o tom, za jakými účely údaje zpracovává, na základě, jakých právních důvodů a o jaké údaje se jedná.
* Je nezbytné určit osobu či útvar, který záznam povede a bude je průběžně aktualizovat. Pokud je u správce či zpracovatele zřízen pověřenec pro ochranu osobních údajů, je vhodné tuto agendu svěřit jemu.
* Aby záznamy byly aktuální, je vhodné všem útvarům správce či zpracovatele uložit povinnost průběžně informovat o změně v jimi prováděných zpracováních. Stejně tak je vhodné, aby pověřenec pro ochranu osobních údajů či jiná osoba, která za záznamy odpovídá, v pravidelných intervalech dotčené útvary vyzývala k potvrzení aktuálnosti, správnosti a úplnosti záznamů o jimi prováděných činnostech zpracování údajů.
* Správce či zpracovatel může vést v záznamech ke každému zpracování evidovat i další informace, aby pro něj záznamy byly využitelnější, např. interní předpis, ve kterém je dané zpracování popsáno, odpovědnou osobu, související produkt, použité IT systémy či aplikace atd.

Záměrná a standardní ochrana osobních údajů

Podle č. 25 GDPR se upravuje povinnost správce postupovat podle dvou spíše koncepčních či právně filosofických principů, kterými jsou záměrná ochrana osobních údajů a standardní ochrana osobních údajů. V praxi používanější a pochopitelnější jsou anglické pojmy Privacy by Design a Privacy by Default.

V případě záměrné ochrany osobních údajů se jedná o zavedení a dokumentování postupu, při němž je správce povinen v okamžiku přípravy nového zpracování osobních údajů či změny stávajícího zpracování (využití dat pro nový účel, změna rozsahu zpracovaných dat, využití nové, invazivnější technologie, např. biometriky apod.).

Postup podle principu standardní ochrany osobních údajů se předpokládá, že správci v rámci každého zpracování přijme taková opatření, aby standardně, jako součást základního nastavení (by Default) byly zpracovány osobní údaje pouze v rozsahu nezbytně nutném pro dosažení daného účelu.

Co si odnést do praxe:

* Správce je povinen zavést principy záměrné a standardní ochrany osobních údajů do všech svých procesů a zdokumentovat, že podle nich v praxi také postupujete.
* V případě záměrné ochrany osobních údajů (Privacy by Design) je vhodné určit klíčové body či již existující procesy pro přípravu nových produktů či procesů a doplnit do nich povinnost již od počátku nastavovat proces či produkt s přihlédnutím k pravidlům pro zpracování osobních údajů.
* Pravidlo standardní ochrany osobních údajů (Privacy by Default) je nutno aplikovat do všech procesů. Správce musí být schopen zdůvodnit a doložit, že základní nastavení zpracování, např. v rámci on-line služby, je z pohledu zásahu do soukromí skutečně minimální.
* Standardní ochrana osobních údajů musí být implementována i do nově připravovaných procesů či produktů, proto je nezbytné nastavit a dokumentovat pravidla pro jeho aplikaci.

Řízení bezpečnostních incidentů

GDPR zavádí na základě čl. 33 a 34 pro každého správce údajů novou povinnost: evidovat, vyhodnocovat a reportovat podle míry rizika pro dotčené osoby Úřadu pro ochranu osobních údajů, v některých případech i dotčeným osobám samým, případy porušení zabezpečení osobních údajů.

Pojem porušení zabezpečení osobních údajů je v GDPR definován jako porušení zabezpečení vedoucí k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.

Incidentem ve smyslu GDPR může být externí útok (úmyslný protiprávní přístup do databáze, krádež smluvní dokumentace, krádež notebooku s klientskou databází, útok na elektronickou službu, který má za následek neoprávněnou změnu či zašifrování dat), interní podvod či jiné protiprávní jednání zaměstnance, technickou chybu, v jejímž důsledku

dojde ke ztrátě dat nebo jejich neoprávněnému zpřístupnění či zveřejnění, například kamerového záznamu či části klientské databáze nebo i nedbalost či nahodilé selhání.

GDPR rozlišuje v zásadě tři úrovně rizika:

* Zanedbatelné či velmi nízké riziko. Takové incidenty je správce povinen evidovat a posoudit, zda je nutno přijmout nápravná opatření, ať už individuální či systémová.
* Nízké a střední riziko. Tyto incidenty je správce povinen evidovat, řešit a také oznámit Úřadu pro ochranu osobních údajů.
* Vysoké riziko. Tyto incidenty je správce povinen evidovat, řešit, oznámit dozorovému orgánu i dotčeným osobám.

V evidenci by tudíž u každého případu **mělo být uvedeno** především:

* Datum a čas prvotního zjištění incidentu.
* Datum a čas jeho interního reportování zaměstnanci či útvaru odpovědnému za hodnocení incidentu a další postup.
* Popis incidentu obsahující především informaci o tom, při kterém procesu se incident stal, a co ho zřejmě způsobilo.
* Popis důsledku incidentu, tzn., zda bylo neoprávněně přistoupeno k osobním údajům, v jakém rozsahu, kterých kategorií údajů se incident týkal atd.
* Základní informace o posouzení rizika a o jeho důvodech, zejména zhodnocení závažnosti incidentu, možného zneužití dat, popisu preventivně přijatých opatření, popisu případně reaktivních opatření atd.
* V případě nutnosti notifikovat rovněž datum, čas a použitý kanál, jak vůči Úřadu pro ochranu osobních údajů, tak dotčeným subjektům.

V případě, kdy správce v konkrétním případu porušení zabezpečení osobních údajů shledá takovou míru rizika, že je nezbytné jej oznámit Úřadu pro ochranu osobních údajů, **MUSÍ TAK UČINIT DO 72 HODIN OD ZJIŠTĚNÍ INCIDENTU**. Tato lhůta se dle obecného výkladu počítá od chvále, kdy správce s alespoň určitou mírou jistoty stanoví, že k incidentu došlo nebo mohlo dojít.

Obrazně řečeno, lhůta nezačíná běžet v okamžiku, kdy pracovník zjistí, že je vylomený zámek u dveří, ani od okamžiku, kdy informační sytém pošle první hlášení o neobvyklé aktivitě uživatele. Pokud má organizace řádně nastavený proces, každý zaměstnanec ví, komu má incident oznámit a učiní tak odpovědné osobě, která se jím bezprostředně začne zabývat. Lhůta tak začíná běžet v okamžiku, kdy tato odpovědná osoba provede prvotní posouzení a dospěje k závěru, že k porušení zabezpečení osobních údajů skutečně mohlo dojít.

Obsahem oznámení o incidentu adresovanému Úřadu pro ochranu osobních údajů musí být:

* 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 správce, které může poskytnout bližší informace.
* Popis pravděpodobných důsledků porušení zabezpečení osobních údajů, zejména pro dotčené osoby, ale i pro další zpracování prováděné organizací, pokud by mohla být z důvodu daného incidentu ohrožena bezpečnost dat obecně.
* 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.

Ať už je správci povinnost informovat o porušení zabezpečení osobních údajů osoby, jejichž údaje byly nebo mohly být incidentem dotčeny, uložena Úřadem pro ochranu osobních údajů, stejně jako v případě, kdy správce sám vyhodnotí incident tak, že pro dotčené osoby představuje vysoké riziko, **toto oznámení by mělo obsahovat v zásadě stejné informace**, jako oznámení zaslané Úřadu pro ochranu osobních údajů vymezené výše.

GDPR správci umožňuje, aby v některých případech, kdy konkrétní případ porušení zabezpečení osobních údajů vyhodnotí jako vysoce rizikové, dotčené osoby neinformoval, a to v těchto situacích:

* Správce zavedl náležitá opatření a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečením osobních údajů. Zejména se jedná o taková opatření, která činí tyto údaje nesrozumitelnými pro kohokoliv, kdo není oprávněn k nim mít přístup, jako je například šifrování, pseudonymizace atd.
* Správce přijal taková následná opatření, která zajistí, e vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví (např. změna všem uživatelů, v přístupových údajích apod.)
* Vyžadovalo by to nepřiměřené úsilí. Taková situace může nastat zejména v případě úniku většího počtu osobních údajů či údajů osob, u kterých správce neeviduje jednoznačné kontaktní údaje a vyžadovalo by dohledání pro správce velmi významnou časovou, kapacitní či finanční zátěž.

Co si odnést do praxe:

* Pro splnění povinností v oblasti porušení zabezpečení osobních údajů je nezbytné nastavit interní eskalační proces, určit odpovědnou osobu.
* Evidenci a posuzování a případné oznamování incidentů dozorovému orgánu a subjektu údajů, kterých se to týká.
* Celý proces eskalace, hodnocení, řešení a reportování incidentů je pro doložení souladu s GDPR nutné dokumentovat.
* Incidenty dle GDPR se hodnotí podle míry rizika pro dotčené osoby, nikoliv pro organizaci samotnou.
* Správce je povinen incident oznámit dozorovému úřadu do 72 hodin po jeho zjištění.
* V evidenci případu porušení zabezpečení osobních údajů je vhodné vést nejen informace o každém jednotlivém incidentu, ale i o procesu jeho vnitřní eskalace, zhodnocení a reportování dozorovému orgánu či dotčeným subjektům.

Ta nudnější část právě skončila!

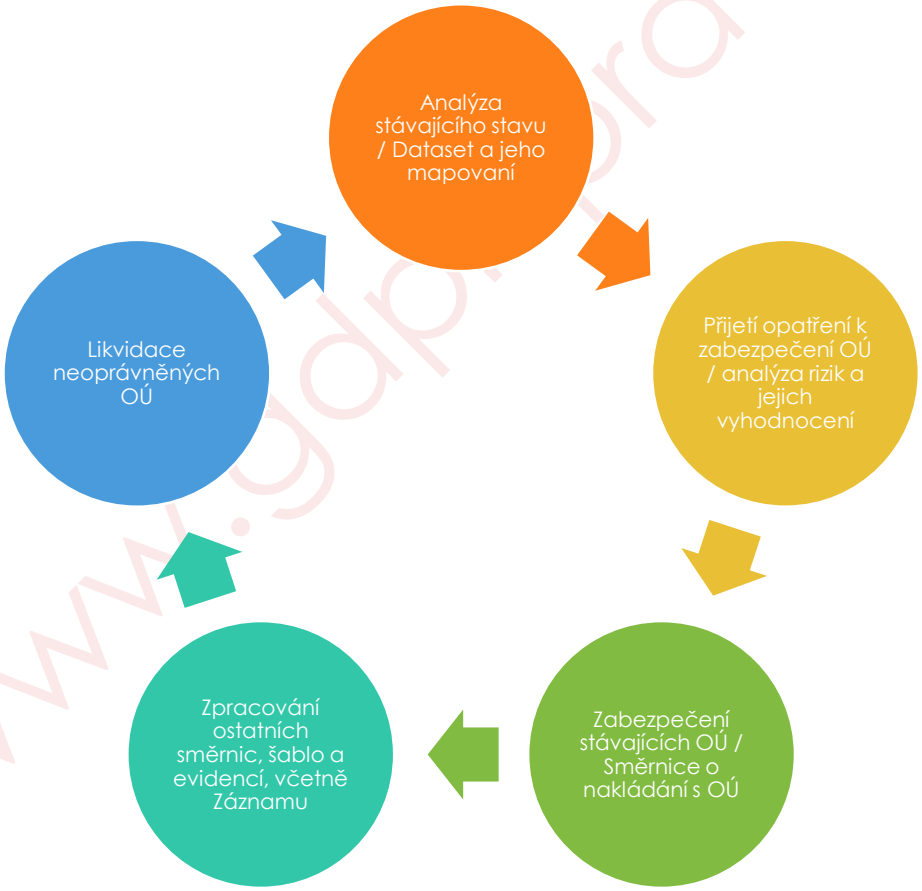
A co bude dál? Nyní se zaměříme na návod, co dělat, a to krok po kroku.

Návod, co dělat – krok za krokem

Následující rady budou jednoduché, dobře zvládnutelné a nákladově nenáročné (v porovnání co platí velké organizace).

V zásadě lze postup shrnout do několika kroků, které probereme v následujících kapitolách podrobněji:

* **Krok 1** Analýza stávajícího stavu
* **Krok 2** Přijetí opatření k zabezpečení osobních údajů
* **Krok 3** Zabezpečení stávajících osobních údajů
* **Krok 4** Zpracování směrnic, šablon, evidencí atd. k tomu pomůže GDPR FG Šablona ™
* **Krok 5** Likvidace nevyhovujících uložišť a „nadbytečných či neoprávněných" osobních údajů



Analýza stávajícího stavu

Analýza jako slovo v sobě obsahuje, že rozebereme celek na jednotlivé části a stále rozkládáme až se dostaneme k jednotlivým základům a poznáme tak souvislosti proč danou činnost konáme, respektive které osobní údaje musíme sbírat a která ne.

Cílem je tedy identifikovat klíčové, důležité a nepodstatné části celku, poznat jejich podstatu, vlastnosti a propojení.

V analýze se zaměříme na Dataset – kde si popíšeme a identifikujeme jednotlivé osobní údaje a kde je vedeme a jaký je důvod. Zároveň si určíte, kam Vám osobní údaje propadávají tzv. flow a na závěr si zpracujete i právní základ nebo chcete-li zda máme zákonný důvod je sbírat a nakládat s nimi.

Abyste mohli zpracovat Dataset je potřeba k němu zdokumentovat směrnici či metodiku, jak to máte provést.

Co je tedy důležité:

* Jak budete zpracovávat – metodika
* Jaké osobní údaje zpracováváte
* V jakých prostorách osobní údaje ukládáte nebo v jakých informačních systémech
* Kdy, kde a jak k těmto osobním údajům přistupujete
* Jaký právní základ osobní údaje mají

Nakládaní s osobními údaji a analýza rizik

V celé organizaci je potřeba definovat **Směrnici pro nakládání s osobními údaji**. Co se stane když, jaký bude eskalační proces, jaká bezpečnostní opatření se provedou nebo jsou již standardem apod. Tato směrnice je jedním z nejdůležitějších dokumentů, abyste mohli zdokumentovat celý proces uvnitř organizace.

Analýza rizik – opět je potřeba vydefinovat metodiku, jak budete analyzovat, jaký algoritmus zvolíte a kdy se incident stane kritickým. Zároveň si vydefinujete. jaká rizika budete měřit (můžete vyjít ze zákonu o kybernetické bezpečnosti nebo přímo z ISO 27005). Následně tyto definice použijete pro analýzu rizik jak pro subjekt údajů, tak pro vaši organizaci a případně navrhnete nová bezpečnostní opatření pro eliminaci rizik.

Směrnice a šablony

Pro správné zdokumentování si stanovíte platné směrnice v souladu s GDPR jako jsou:

* Metodika mapovaní datasetu
* **Metodika analýzy rizik**
* Spisový a skartační řád
* Specifikace požadavků na systémy
* **Pravidla pro nakládání s informacemi**
* **Registr porušení**

* **Záznam o zpracování**
* Smlouva se zpracovateli
* **Prohlášení o aplikovatelnosti**
* Požadavek subjektu na přístup
* Souhlas se zpracováním
* Souhlas se zpracováním u dětí
* Odvolání souhlasu
* Odvolání souhlasu dětí

Likvidace

Zlikvidujete vše, co nepotřebujete a tím myslíme, nevhodné nosiče, média i zálohy s daty, k jejichž uchovávání nebudete mít oprávnění – pamatujte, že je potřeba MINIMALIZOVAT.

V návaznosti na provedenou analýzu Datasetu a Analýzy rizik odstraňte všechna nadbytečné a nepotřebné osobní údaje z míst, která nejsou řádně zabezpečena a samozřejmě která máte v rozporu s vašimi právními požadavky.

Záznamy o činnostech zpracování osobních údajů a četnosti

Jak již bylo popsáno v předchozích kapitolách je potřeba tyto záznamy uchovávat v písemné formě (papírově nebo elektronicky) a aktuální podobě, ale co to je aktuální podoba? Každý týden, měsíc nebo rok? Neexistuje doporučení, která se dá použít pro všechny, ale orientačně se dá říct:

* Minimálně 1x za rok udělat Záznam o zpracován osobních údajů pro malé organizace, Pro střední a velké kvartálně.
* Udělat záznam, pokud změníte účel nebo cíl zpracování osobních údajů v zásadě Privacy by Design.
* Se záznamem je potřeba udělat Analýzu rizik a mapování datasetu.
* Minimálně 1x ročně revize všech směrnic – netvrdíme, že se musí měnit, ale musí vždy být v aktuální verzi a popisovat skutečnost u Vás.

Závěr

Věříme, že jsme dokázali shrnout to nejdůležitější z GDPR do kratší a srozumitelnější verzi.

Teď už víte, jaké povinnosti vás čekají a co je potřeba udělat, abyste byli v souladu s GDPR, které vstoupí v platnost 25. května 2018.

Pokud máte pocit, že byste potřebovali přece jenom více informací nebo se nastartovat pomocí metodických šablon jsme Vám připraveni pomoci **GDPR FG Šablona ™**, která obsahuje:

Mapování:

* Metodika mapování
* Šablona mapování účelu a použití

Bezpečnost:

* Analýza rizik
* Seznam rizik
* Metodika analýzy rizik

Práva subjektů:

* Spisový a skartační řád
* Specifikace požadavků na systémy
* Pravidla pro nakládání s informacemi

Právo:

* Registr porušení
* Záznam o zpracování
* Smlouva se zpracovateli
* Prohlášení o aplikovatelnosti
* Požadavek subjektu na přístup
* Souhlas se zpracováním
* Souhlas se zpracováním u dětí
* Odvolání souhlasu
* Odvolání souhlasu dětí

Máte-li zájem o tyto šablony nebo i jiné a případně další informace, jsou pro Vás připraveny.