ARBONIA

Pokyn týkající se zacházení s údaji (pokyny z bezpečnosti údajů)

16. června 2020

ARBONIA

OBSAH

ARBONIA

1 ÚČEL A CÍL

Pro plnění zákonných a smluvních povinností je nezbytné shromažďovat a zpracovávat osobní údaje. Přitom musí být v příslušných zemích přísně dodržovány platné předpisy o ochraně osobních údajů. Předkládaný pokyn dokládá, jak společnost Arbonia AG a její koncernové společnosti (dále společně "Arbonia", nebo jednotlivá koncernová společnost dále jen "koncernová společnost") zacházejí s osobními údaji. Stanovená ustanovení platí jako minimální standardy. Pokud místní zákon o ochraně osobních údajů stanoví přísnější pravidla, musí být dodržována. Také je třeba dodržovat všechna místní pravidla pro provádění předkládaného pokynu.Účelem tohoto pokynu o zacházení s údaji ("Pokyn k ochraně osobních údajů") je stanovit, provádět, udržovat a neustále zlepšovat dodržování ochrany údajů v souladu s požadavky obecného nařízení o ochraně osobních údajů Evropské unie 2016/679 (GDPR) a všech dalších platných místních zákonů o ochraně osobních údajů (souhrnně **použitelné zákony o ochraně osobních údajů**) společností Arbonia.

Nedodržením použitelných zákonů o ochraně osobních údajů se vystavuje společnost Arbonia riziku poškození pověsti a přísným pokutám (např. až 4 % celosvětového obratu podle GDPR). Navíc může vystavit naše zákazníky a zaměstnance určitým rizikům v oblasti ochrany údajů, jako je krádež identity nebo finanční ztráty. Dodržování použitelných zákonů o ochraně osobních údajů nám pomáhá udržet důvěru v organizaci Arbonia a zajistit úspěšné obchodní operace.

Cílem tohoto pokynu k ochraně osobních údajů je poskytnout rámec pro takové dodržování uvnitř společnosti Arbonia. Jeho cílem je zejména zavést základní zásady pro zpracování osobních údajů (**zásady ochrany údajů**) stanovené v odstavci 6, a za které společnosti Arbonia odpovídají, pokud jednají jako odpovědné osoby podle GDPR, upravovat potřebu vhodných technických a organizačních opatření a hlášení incidentů v oblasti ochrany údajů jako minimální standard pro všechny společnosti Arbonia. Tento pokyn platí pro všechny pracovníky společnosti Arbonia a členy správní rady společnosti Arbonia AG.

Dále poskytuje rámec pro další požadavky, které platí pro odpovědné osoby a zpracovatele objednávky podle nařízení o GDPR (nebo podobných platných zákonů o ochraně osobních údajů), jak je popsáno v odstavci 7.

2 POJMY A DEFINICE

Pro účely těchto pokynů k ochraně osobních údajů platí následující pojmy a definice:

Anonymizovaná data znamenají, že osobní identitu nemůže nikdo vysledovat nebo že osobní identitu lze vysledovat pouze s vynaložením nepřiměřeného času, nákladů a úsilí.

Použitelné zákony o ochraně osobních údajů jsou předmětem obecného nařízení o ochraně osobních údajů Evropské unie 2016/679 (**GDPR**) nebo jiných použitelných národních zákonů o ochraně osobních údajů, které obsahují podobná ustanovení.

Vlastník obchodního procesu je zkratkou pro fyzickou osobu, která je podle těchto pokynů k ochraně osobních údajů odpovědnou osobou a je odpovědná za zpracování osobních údajů a příslušné IT aplikace.

Souhlasem se rozumí souhlas dotčených osob, tedy každé osoby dobrovolně pro určitý případ, informovaným způsobem a srozumitelně vyjádřeným projevem vůle ve formě prohlášení nebo jiného jednoznačného potvrzujícího jednání, kterým dává dotčená osoba najevo, že souhlasí se zpracováním osobních údajů, které se na ni vztahují.

Odpovědná osoba je fyzická nebo právnická osoba, úřad, agentura nebo jiný subjekt, který určuje účely a prostředky zpracování osobních údajů samostatně nebo společně s ostatními.

Incident v oblasti zabezpečení údajů zahrnuje událost, u které existuje oprávněné podezření, že u osobních údajů došlo protiprávně k jejich evidenci, shromažďování, změnám, kopírování, přenášení a používání. To se může vztahovat na jednání třetích stran nebo zaměstnanců.

Dotčená osoba je identifikovaná nebo identifikovatelná fyzická osoba. Identifikovatelná fyzická osoba je osoba, kterou lze přímo nebo nepřímo identifikovat, zejména spojením s identifikátorem, jako je jméno, identifikační číslo, lokalizační údaje, online identifikátor nebo jedna nebo více specifických vlastností, které jsou vyjádřením fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity této fyzické osoby.

Zpracovatel objednávky je fyzická nebo právnická osoba, úřad, zařízení nebo jiný subjekt, který zpracovává osobní údaje jménem odpovědné osoby.

Seznam operací zpracování je záznamem o zpracování údajů, za který odpovídá odpovědná osoba. Tento seznam obsahuje veškeré následující údaje: (i) jméno a kontaktní údaje odpovědné osoby a případně společné odpovědné osoby, zástupce odpovědné osoby a místního koordinátora ochrany údajů; (ii) účely zpracování; (iii) popis kategorií dotčených osob a kategorie osobních údajů; (iv) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích; (v) případně předávání osobních údajů do třetí země, včetně uvedení třetí země a dokumentace vhodných záruk; (vi) předpokládané lhůty pro výmaz různých kategorií osobních údajů; (vii) obecný popis technických a organizačních bezpečnostních opatření.

Inspektor ochrany osobních údajů nebo koordinátor ochrany osobních údajů nebo DSK platí pro osobu popsanou v odstavci 5.

Osobními údaji se rozumí veškeré informace (včetně osobních údajů zvláštních kategorií) týkající se dotčené osoby, tedy informace týkající se identifikované nebo identifikovatelné fyzické osoby, jako je jméno, datum narození, e-mailová adresa, náboženství, údaje o poloze, online údaje (IP adresa, údaje o poloze atd.), identifikační čísla (číslo sociálního pojištění, číslo průkazu totožnosti atd.), fyzické vlastnosti (pohlaví, kůže, vlasy, barva očí atd.), údaje o zákaznících atd.), které podléhají platnému nařízení o ochraně osobních údajů.

Zpracováním se rozumí jakákoli operace nebo řada operací prováděných s pomocí nebo bez pomoci automatizovaných postupů v souvislosti s osobními údaji, jako je shromažďování, evidence, organizace, objednávání, ukládání, přizpůsobení nebo modifikace, čtení, dotazování, použití, zveřejnění přenosem, šíření nebo jakákoli jiná forma poskytování, srovnávání nebo propojení, omezení , výmazu nebo zničení.

Pseudonymizací se rozumí zpracování osobních údajů takovým způsobem, že osobní údaje již nemohou být přiděleny konkrétní dotčené osobě bez použití dodatečných informací za předpokladu, že tyto dodatečné informace jsou uchovávány odděleně a podléhají technickým a organizačním opatřením, která zajistí, že osobní údaje nebudou přiděleny identifikované nebo identifikovatelné fyzické osobě.

Osobními údaji zvláštních kategorií se rozumí údaje o rasovém nebo etnickém původu, politických názorech, náboženských nebo filozofických názorech, odsouzení za trestný čin, členství v odborech, zdraví nebo sexuální orientace dotčené osoby nebo genetické údaje, biometrické údaje pro účely jedinečné identifikace fyzické osoby.

Třetí země jsou všechny státy, které nejsou zeměmi Evropské unie nebo Evropského hospodářského prostoru nebo zeměmi s odpovídající úrovní ochrany údajů, kterou Evropská komise považuje za vhodnou (viz seznam zemí s odpovídající úrovní ochrany údajů: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Třetí strana zastupuje kohokoli jiného než dotčenou osobu, odpovědnou osobu nebo zpracovatele objednávky (včetně obchodních partnerů, subdodavatelů, agentur pro podávání zpráv o úvěrech a dalších), jakož i osoby, které jsou oprávněny zpracovávat osobní údaje pod přímou pravomocí oprávněné osoby nebo zpracovatele objednávky. Při zpracování osobních údajů na základě povolení nejsou zpracovatelé objednávky právně žádné třetí subjekty podle zákona o ochraně osobních údajů, protože jsou právně přidělováni odpovědné osobě.

3 ROZSAH

3.1 Organizační rozsah

Tento pokyn k ochraně osobních údajů se vztahuje na všechny společnosti skupiny Arbonia, na všechny pracovníky společnosti Arbonia a na členy správní rady Arbonia AG. Tento pokyn je právně závazný pro všechny koncernové společnosti.

3.2 Zákony, ustanovení, standardy a pokyny

Tato směrnice o ochraně údajů se vztahuje na požadavky nařízení GDPR a mezinárodně uznávaných zásad ochrany údajů, aniž by nahradila stávající národní právo. Nahrazuje národně použitelné zákony o ochraně osobních údajů. Příslušné národní právo má přednost v případě rozporu s tímto pokynem k ochraně osobních údajů nebo v případě přísnějších požadavků, než je tento pokyn k ochraně osobních údajů. Obsahy tohoto pokynu k ochraně osobních údajů musí být rovněž dodrženy, pokud neexistují odpovídající státní právní předpisy.

Pokud je tento pokyn k ochraně osobních údajů v rozporu s ustanoveními určité země, mohou být zvláštní ustanovení tohoto pokynu k ochraně osobních údajů převzata místním pokynem po dohodě s Head Legal & Compliance. Základní obsahy a účel dotyčných ustanovení však nesmí být měněn.

4 REGULAČNÍ ZÁKLAD

Tento pokyn k ochraně osobních údajů je založen na GDPR a celosvětově uznávaných základních zásadách ochrany údajů.

5 ROLE A ODPOVĚDNOSTI

- Jednatel koncernové společnosti[1] je odpovědný za následující:
  1. v konečném důsledku zajistit, aby příslušná právnická osoba plnila své právní povinnosti týkající se zpracování osobních údajů.
  2. zajistit, aby byly splněny požadavky tohoto pokynu k ochraně osobních údajů (včetně oznamování incidentů v oblasti bezpečnosti údajů).
  3. zajistit, aby vlastník obchodního procesu vyplnil a udržoval "seznam zpracovatelských operací" na úrovni koncernové společnosti.
  4. Určit formálního místního inspektora ochrany osobních údajů (interního nebo externího) (dále jen "inspektora ochrany osobních údajů"), pokud to vyžaduje příslušné místní nařízení o ochraně osobních údajů, a tuto jmenovanou osobu každoročně v polovině roku oznámit Head Legal & Compliance a Internal Audit.
  5. určit místního správce ochrany osobních údajů (dále jen "koordinátor ochrany osobních údajů"), pokud příslušné místní nařízení o ochraně údajů nevyžaduje formálního místního inspektora ochrany údajů. Tuto jmenovanou osobu oznámit v polovině roku Head Legal & Compliance a Internal Audit.

[1] Za koncernové společnosti, které nejsou operativně činné, je tato odpovědnost stanovena samostatně po konzultaci s Head Legal & Compliance.

- Místní koordinátor ochrany osobních údajů, resp. inspektor ochrany osobních údajů, jmenovaný jednatelem koncernové společnosti[2] musí:
  1. sledovat dodržování tohoto pokynu k ochraně údajů a pokynů odpovědné osoby nebo zpracovatele objednávky, pokud jde o ochranu osobních údajů, včetně přenosu kompetencí a odpovídajích auditů.
  2. informovat, poskytovat rady a dozor odpovědnému pracovníkovi nebo zpracovateli objednávky a zaměstnancům, kteří uskutečňují povinnosti v souladu s tímto pokynem k ochraně osobních údajů.
  3. na požádání poskytovat poradenství ohledně posouzení dopadů na ochranu osobních údajů a kontrolovat jejich výsledky, jakož i odpovídat na další otázky týkající se osobních údajů, které mu byly přiděleny podle těchto pokynů k ochraně osobních údajů.
  4. udržovat "adresář zpracovatelských operací", který je řízen příslušnou koncernovou společností a vyplňován vlastníky obchodních procesů, kontrolovat, aktualizovat a ročně k polovině roku potvrzovat úplnost a aktuálnost seznamu pro jednatele a Head Legal & Compliance.
  5. sloužit jako kontaktní místo pro Head Legal & Compliance, průběžně informovat o odpovědnosti, rizicích a problémech týkajících se ochrany osobních údajů.
  6. Podporovat IT, které je odpovědné za IT aplikaci, při kontrole a schvalování nových IT aplikací na úrovni koncernové společnosti pro zpracování osobních údajů a veškerých IT aplikací pro zpracování zvláštních kategorií osobních údajů z hlediska ochrany údajů.
  7. ¨schvalovat předávání osobních údajů do třetí země z hlediska ochrany údajů (viz také níže, čís. 14).
  8. sloužit jako místní kontaktní místo pro orgán dozoru v otázkách zpracování údajů a spolupracovat s orgánem dozoru;
  9. Vyřizovat žádosti zaměstnanců zapojených do procesu zpracování osobních údajů.
  10. reagovat na žádosti dotčených osob o informace o osobních údajích, které má od nich společnost Arbonia ve svém vlastnictví, nebo reagovat na dotazy k většímu počtu koncernových společností Arbonia v koordinaci s Corporate IT (viz také čís. 7.4)
  11. Přezkoumat a schválit smlouvy vypracované, resp. předem zkontrolované vlastníkem obchodního procesu, nebo dohody se zpracovatelem objednávky, kteří mohou zpracovávat osobní údaje jménem společnosti Arbonia, jak je uvedeno v odstavci 7.2.
  12. kontrolovat externího místního inspektora ochrany údajů, pokud byl takový jmenován.
  13. hlásit incidenty v oblasti bezpečnosti údajů podle pokynu Data Breach Notification (viz násl. č. 9 jakož i „Arbonia Data Breach Policy“).

[2] Za koncernové společnosti, které nejsou operativně činné, je tato odpovědnost stanovena samostatně po konzultaci s Head Legal & Compliance.

- IT-Board společně s Corporate IT je odpovědný za následující:
  1. definovat platné standardy pro celý koncern, jakož i základní kontroly IT (GITC), které je třeba při ukládání údajů dodržovat.

- příslušné oddělení IT, které se stará o koncernovou společnost, je odpovědné za následující:
  1. prostřednictvím vhodných norem, zabezpečením a prováděním základních kontrol IT (GITC) zajistit, aby systémy, služby a vybavení používané k ukládání údajů, splňovaly přijatelné bezpečnostní standardy (kontrola přístupu / výmaz údajů), přičemž je třeba respektovat stav techniky, náklady na realizaci a charakter, rozsah, souvislosti a účel zpracování, jakož i různé pravděpodobnosti a závažnosti dopadu na práva a svobody fyzických osob.
  2. usilovat o to, aby odpovědná osoba a zpracovatel objednávky provedli vhodná technická a organizační opatření k zajištění úrovně ochrany odpovídající riziku, jak je stanoveno v odstavci 8.
  3. po konzultaci s koordinátorem ochrany údajů nebo inspektorem ochrany osobních údajů přezkoumat a schválit nové IT aplikace pro zpracování osobních údajů z hlediska ochrany údajů.
  4. provádět pravidelné kontroly a skeny, abyste se zajistilo, že bezpečnostní hardware a software pracují správně. Výsledky kontrol ochrany údajů musí být oznámeny odpovědnému inspektorovi ochrany údajů.
  5. vyhodnotit zabezpečení dat všech služeb třetích stran (např. zpracovatelů objednávky), které společnost bere v úvahu pro zpracování osobních údajů (např. služby cloud computingu atd.)
  6. Udržovat seznam incidentů v oblasti zabezpečení dat a nahlásit incidenty v oblasti zabezpečení dat Corporate IT.
  7. koordinovat a zodpovídat žádosti dotčených osob podle informací o jejich osobních údajích, které vlastní koncernová společnost Arbonia, spravovaná příslušným IT oddělením (viz také násl. čís. 7.4)
  8. hlásit incidenty nebo rizika v oblasti bezpečnosti údajů analogicky s pokynem Data Breach Notification (viz násl. č. 9 jakož i „Arbonia Data Breach Policy“)

- Corporate IT ve spolupráci s oddělením IT, které je odpovědné za jednu koncernovou společnost: Zodpovídá za následující:
  1. provádět pravidelné kontroly a skeny, abyste se zajistilo, že bezpečnostní hardware a software pracují správně. Výsledky kontrol ochrany údajů musí být oznámeny odpovědnému inspektorovi ochrany údajů.
  2. Udržovat centrální seznam incidentů v oblasti zabezpečení dat.
  3. hlásit incidenty nebo rizika v oblasti bezpečnosti údajů analogicky s pokynem Data Breach Notification (viz násl. č. 9 jakož i „Arbonia Data Breach Policy“).

- interní audit odpovídá za následující:
  1. zkontrolovat při příležitosti auditů prováděných v souladu s pravidelným plánováním auditů v rámci kontroly založené na posouzení rizik, zda organizační postupy odpovídají základním požadavkům tohoto pokynu k ochraně údajů.

- vlastník obchodního procesu je odpovědný za následující:
  1. zajistit, aby byl místní inspektor ochrany údajů přiměřeně a včas zapojen do všech dotazů nezbytných pro posouzení zpracování osobních údajů.
  2. vyhotovit, popř. předem zkontrolovat všechny smlouvy, nebo dohody se zpracovatelem objednávky, zpracovat osobní údaje jménem společnosti Arbonia, jak je uvedeno v odstavci 7.2.
  3. vyplňovat "adresář zpracovatelských operací", který je řízen příslušnou koncernovou společností a udržovat ho v aktuálním stavu, a ročně ke konci dubna potvrzovat úplnost a aktuálnost záznamů koordinátorovi ochrany dat, resp. inspektorovi ochrany dat.
  4. Před implementací nových operací zpracování osobních údajů posoudit z toho vyplývající rizika pro osobnost a základní práva dotčené osoby, a v případě vysoce pravděpodobného rizika zpracování, předem provést posouzení dopadu na ochranu údajů.

6 ZÁSADY OCHRANY ÚDAJŮ PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Každá koncernová společnost jednající jako odpovědná osoba při zpracování osobních údajů musí zajistit, aby bylo možné prokázat soulad s následujícími **6 (šesti) základními zásadami ochrany údajů:**

1. zpracovávat výhradně osobní údaje, pokud je platný právní základ prokázán podle platných zákonů o ochraně údajů, a dotčená osoba může být informována o totožnosti a kontaktních údajích odpovědné osoby, o způsobu a právních základech evidovaných osobních údajů, o příslušných lhůtách ukládání a o účelu, za kterým byla osobní data evidována

2. je třeba vždy respektovat účel, pro který byly osobní údaje pořízeny

3. Pořizovat/zpracovávat pouze takové osobní údaje, které jsou skutečně zapotřebí

4. Udržovat osobní údaje korektně a nesprávné osobní údaje vymazat

5. Uchovávat osobní údaje pouze po dobu, která je dle zákona skutečně nezbytná

6. S osobními údaji je třeba zacházet v tajnosti a sdělovat pouze to, co je skutečně třeba sdělovat

6.1 Spravedlnost, zákonnost a transparentnost

Osobní údaje mohou být zpracovávány pouze pro účely výslovně povolené, jak je popsáno níže; toto musí být provedeno transparentním způsobem. Osobní údaje musí být proto zpracovávány zákonným a spravedlivým způsobem a musí být respektována individuální práva dotčené osoby. To může zahrnovat osobní údaje, které společnost Arbonia obdrží přímo od dotčené osoby (například vyplněním formulářů nebo naší společnou korespondencí poštou, telefonicky, e-mailem nebo jinak), jakož i osobní údaje, které společnost Arbonia obdrží od třetích stran.

Podle platných zákonů o ochraně osobních údajů mohou být osobní údaje zpracovávány zákonně na základě jednoho z **pěti legitimních důvodů** (**právních důvodů**) podle GDPR. Tyto důvody zahrnují následující:

1. **Smlouva**: Zpracování osobních údajů je nezbytné pro plnění smlouvy, jejíž smluvní stranou je dotčená osoba, nebo pro provádění předsmluvních opatření přijatých na žádost dotčené osoby, nebo

2. **Souhlas:** Zpracování osobních údajů je založeno na souhlasu (modelu Opt-in) dotčené osoby pro jeden nebo více specifických účelů. Souhlas musí být dokumentován, nebo

3. **Právní povinnost:** Zpracování osobních údajů je založeno na právní povinnosti společnosti Arbonia. Povaha a rozsah zpracování údajů musí být nezbytné pro právně přípustnou činnost zpracování a musí být dodrženy platné právní podmínky, nebo

4. **Veřejný zájem:** Zpracování je nezbytné pro plnění úkolu, který je ve veřejném zájmu, nebo

5. **Oprávněné obchodní zájmy:** Zpracování je úměrné vzhledem k oprávněným obchodním zájmům společnosti Arbonia nebo třetí strany, které jsou osobní údaje sdělovány, pokud zájmy nebo základní práva a základní svobody dotčené osoby tyto zájmy nepřeváží. Oprávněné zájmy jsou obecně právního (např. vymáhání nesplacených pohledávek / kolektivní smlouvou se závodní radou / uplatněním / výkonem nebo obhajobou proti právním nárokům vůči dotčené osobě) nebo obchodního charakteru (např. zabránění porušování smlouvy).

Transparentnost vyžaduje, aby byla dotčená osoba informována o tom, jak je nakládáno s jejími osobními údaji. Obecně se proto doporučuje pořizovat osobní údaje přímo od dotčené osoby (a nikoli prostřednictvím třetí strany). Pokud dojde ke zpracování osobních údajů, je třeba dotčenou osobu informovat o následujících skutečnostech:

- o jménu a kontaktních údajích odpovědné osoby, jakož i eventuálně jejího zástupce v EU
- eventuálně o kontaktních údajích koordinátora ochrany údajů, resp. inspektora ochrany údajů
- o účelu zpracování osobních údajů, jakož i o právních základech pro zpracování
- o třetím příjemci, nebo kategoriích třetích příjemců, kterým mohou být údaje zprostředkovány
- Pokud to připadá v úvahu, informace ke zpracování ve třetí zemi a odkaz na přiměřené záruky

6.2 Účelové omezení

Osobní údaje mohou být zpracovávány pouze za účelem sděleným dotčené osobě před shromažďováním osobních údajů. Následné změny účelu jsou možné pouze v omezené míře a vyžadují odůvodnění. Odpovědná osoba musí informovat dotčenou osobu o účelu, pro který Arbonia zpracovává její osobní údaje, pokud společnost Arbonia pořizuje osobní údaje poprvé nebo co nejdříve poté. Při jakémkoli zpracování pro reklamní účely nebo pro marketingové programy musí být dotčené osobě uděleno právo na námitku proti zpracování jejích osobních údajů a musí být o této skutečnosti výslovně informována. V tomto ohledu musí každá odpovědná osoba provést vyřizování stížností, které zajistí, že se bude respektovat Opt-Outs.

6.3 Minimalizace údajů

Zpracovávat pouze takové osobní údaje, které jsou skutečně zapotřebí Před zpracováním osobních údajů je nutné určit, zda a do jaké míry je zpracování osobních údajů nezbytné k dosažení uskutečňovaného účelu. Osobní údaje nesmějí být shromažďovány předem a uchovávány pro potenciální budoucí účely, pokud to nevyžaduje nebo nepovoluje národní právo.

6.4 Správně a aktuálně

Osobní údaje musí být udržovány správné, úplné a - pokud dojde ke změnám - aktuální. Musí být přijata vhodná opatření, aby bylo zajištěno, že nepřesné nebo neúplné osobní údaje budou vymazány, opraveny, doplněny nebo aktualizovány. Každý, kdo pracuje s osobními údaji, musí učinit přiměřené kroky (například potvrzením údajů dotčené osoby, pokud tato zavolá, či odstraněním uloženého telefonního čísla z databanky, když je dotčená osoba již nepoužívá).

6.5 Omezená doba uchovávání

Osobní údaje se smějí uchovávat pouze po skutečně potřebnou dobu uchovávání. Osobní údaje musí být vymazány, jakmile již nejsou nezbytné pro zamýšlené účely, nebo je souhlas odvolán nebo je vznesena námitka, nebo vznikl rozpor na základě oprávněného zájmu a společnost Arbonia nemůže uvést žádné přednostní oprávněné důvody. V některých

případech nám delší doby uchovávání mohou umožnit uchovávat osobní údaje po delší dobu, pokud to vyžaduje zákon (např. podle daňových a obchodních zákonů), nebo mohou být osobní údaje vyžadovány pro uplatnění, výkon, nebo obhajobu právních nároků.

6.6 Důvěrnost a bezpečnost údajů

S osobními daty je třeba zacházet vždy v tajnosti a sdělovat pouze to, co je skutečně třeba sdělovat. Platí zde zásada "požadovaných informací", takže zaměstnanci a třetí subjekty mají přístup k osobním údajům pouze v rozsahu nezbytném pro splnění účelu. To vyžaduje pečlivě vytvořený koncept, který definuje konkrétní přístupová práva pro každou obchodní transakci, včetně realizace a schvalování rolí a odpovědností (koncepce přístupových práv). Příjemci osobních údajů musí být informováni o důvěrnosti osobních údajů a **musí se podrobit dohodě o zachování mlčenlivosti/dohodě o zachování důvěrnosti** (která může být součástí pracovní smlouvy apod.). Výjimka: Příjemce podléhá profesní nebo zákonné povinnosti mlčenlivosti.

Osobní údaje musí být zabezpečeny vhodnými organizačními a technickými opatřeními, aby se zabránilo neoprávněnému přístupu, nezákonnému zpracování nebo zveřejnění, jakož i neúmyslné ztrátě, změně nebo zničení (viz odstavec 8).

7 DALŠÍ POVINNOSTI PODLE GDPR NEBO JINÝCH PODOBNÝCH PLATNÝCH NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

7.1 Zásada odpovědnosti

Koncernová společnost Arbonia, která podléhá GDPR (nebo podobnému platnému nařízení o ochraně údajů), musí zajistit, aby mohla prokázat dodržování platných zákonů na ochranu údajů (zásada "odpovědnosti"). Proto musí tyto koncernové společnosti kromě obecných požadavků podle tohoto pokynu k ochraně údajů realizovat a zachovávat následující body, přičemž jednatel příslušné koncernové společnosti musí v konečném důsledku zajistit realizaci a zachování:

1. místní koordinátor ochrany osobních údajů nebo místní inspektor ochrany osobních údajů: Jmenovat specializovaného místního koordinátora ochrany osobních údajů nebo inspektora ochrany osobních údajů

2. vedení "adresáře operací zpracování": Soupis činností zpracování osobních údajů": Je třeba vést a aktuálně udržovat inventář aktivit zpracování osobních údajů.

3. Ověření legitimnosti: Zákonné zpracování osobních údajů v souladu s platnými právními důvody musí být kontrolováno, zejména při zpracování zvláštních kategorií osobních údajů

4. Kontrola zpracovatele objednávky: Uzavření smlouvy o zpracování se zpracovatelem nebo jako zpracovatel při poskytování nebo příjmu osobních údajů na základě povolení podle článku 28 GDPR.

5. Pokud zpracování provádí více odpovědných osob společně, předpokládá se dohoda mezi těmito odpovědnými osobami podle článku 26 GDPR.

6. Zaměstnance společnosti Arbonia je třeba informovat o činnosti v souvislosti se zpracováním osobních údajů.

7.2 Pravidla pro zpracovatele objednávky (především servisní partnery)

Odpovědná osoba spolupracuje pouze se zpracovateli objednávky, kteří poskytují dostatečné záruky, že budou přijata vhodná technická a organizační opatření tak, aby zpracování osobních údajů probíhalo v souladu s požadavky článku 28 GDPR a zajistilo ochranu práv dotčené osoby.

V případě sdílených služeb v rámci společnosti Arbonia existuje dohoda, která umožňuje přenos osobních údajů, pokud existují právní důvody pro přenos těchto osobních údajů v souladu s platnými zákony na ochranu údajů.

7.2.1 Poskytování osobních údajů zpracovateli objednávky (odchozí)

Zpracování osobních údajů na základě jednoho povolení znamená, že poskytovatel služeb je pověřen zpracováním osobních údajů, bez odpovědnosti za příslušný obchodní postup (tj. poskytovatelé služeb, outsourcingové služby). V takovém případě musí být smlouva o zpracování objednávky na zpracování osobních údajů uzavřena s externími poskytovateli na základě povolení. Příslušná koncernová společnost Arbonia je odpovědnou osobou a nese plnou odpovědnost za správné provedení zpracování osobních údajů zpracovatelem objednávky.

Příslušný vlastník obchodního procesu musí zajistit, aby byl pro zpracování objednávek použit aktuální model dohody nebo podobná smlouva poskytnutá poskytovatelem služeb, aby se splnily požadavky vyplývající z článku 28 GDPR, aby bylo možné tyto poskytovatele služeb pověřit provedením objednávky. Poskytovatel služeb může také alternativně dokumentovat dodržování požadavků na bezpečnost údajů předložením vhodné a schválené certifikace EU. Každá odchylka od takového bezpečnostního standardu musí být schválena inspektorem ochrany osobních údajů nebo koordinátorem ochrany osobních údajů ve spolupráci s Corporate IT. Stávající smlouvy musí být přepracovány do jednoho roku od vstupu tohoto pokynu o ochraně údajů v platnost a musí obsahovat písemnou smlouvu o zpracování objednávky.

7.2.2 Příjem osobních údajů jako zpracovatel objednávky (podrobně)

Pokud osobní údaje předává koncernové společnosti Arbonia třetí strana, je nutné zajistit, aby osobní údaje (i) mohly být použity k určenému účelu, (ii) shromažďovány na základě oprávněných důvodů (doporučuje se vyžádat si písemné potvrzení) a (iii) aby existovala smlouva o zpracování objednávek, která je v souladu s článkem 28 GDPR.

7.3 Přeshraniční předávání osobních údajů

V případě přeshraničního předávání osobních údajů musí být splněny příslušné národní požadavky na zveřejnění osobních údajů v zahraničí. Podle GDPR může k předávání osobních údajů docházet v rámci EU, EHP nebo do země, o které Evropská komise zjistila, že tato země splňuje odpovídající záruky, aby byla zajištěna odpovídající úroveň ochrany údajů. Takové předávání údajů nepodléhá žádnému zvláštnímu druhu schvalování. Evropská komise mimo jiné zařadila Švýcarsko jako zemi poskytující odpovídající ochranu (viz aktuální seznam zemí:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Předávání osobních údajů do třetí země je povoleno pouze tehdy, jsou-li k dispozici další odpovídající záruky. To znamená, že pokud může příjemce prokázat, že dodržuje standard ochrany údajů, který tomuto pokynu ochrany údajů odpovídá (např. i), předložení závazných podnikových pravidel, ii) uzavření standardních smluvních doložek EU pro zpracování objednávek ve třetích zemích s poskytovatelem služeb a jinými subdodavateli ,[3] iii) zavedení pravidel chování schválených orgánem dozoru, iv) účast poskytovatele služeb na certifikačním systému akreditovaného EU pro dosažení dostatečné úrovně ochrany údajů, nebo v) individuální dohody mezi odpovědnou osobou a zpracovatelem objednávky na základě povolení příslušného orgánu dozoru) a informace pro dotčenou osobu. Tato povinnost neplatí, pokud je předávání založeno na právní povinnosti. Takové předávání vyžaduje souhlas koordinátora ochrany údajů nebo inspektora ochrany údajů.

Pokud jsou osobní údaje předávány v rámci společnosti Arbonia, je koncernová společnost importující osobní údaje povinna, spolupracovat se všemi žádostmi příslušného orgánu dozoru v zemi, kde má exportující koncernová společnost své sídlo, a vyhovět všem připomínkám příslušného orgánu dozoru v souvislosti se zpracování předávaných osobních údajů.

7.4 Zacházení s žádostí o informace od dotčené osoby

Dotčené osoby mají právo podat formální žádost o informace o podrobnostech osobních údajů, které společnost Arbonia vlastní a mohou požadovat následující:

[3] Viz Rozhodnutí komise z 5. února 2010 standardních smluvních doložkám pro předávání osobních údajů zpracovateli objednávky ve třetích zemích podle směrnice 95/46/EU Evropského parlamentu a rady, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

Právo na informace o:

- účelech zpracování;
- kategoriích osobních údajů, které se zpracovávají;
- příjemcích nebo kategoriích příjemců, kterým osobní údaje byly nebo ještě jsou poskytovány, zejména příjemcům ve třetích zemích nebo v mezinárodních organizacích;
- pokud je to možné, o plánované době, po kterou budou osobní údaje ukládány, nebo, pokud to není možné, o kritériích pro stanovení této doby;
- existenci práva na opravu nebo výmaz příslušných osobních údajů, nebo omezení zpracování odpovědnou osobou nebo práva vznést námitku proti takovému zpracování;
- existenci práva na stížnost u orgánu dozoru
- veškerých dostupných informacích o původu údajů, pokud nebyly osobní údaje pořízeny od dotčených osob;
- existenci automatizovaného rozhodování, včetně profilingu;
- Jsou-li osobní údaje předávány do třetí země nebo mezinárodní organizaci, má dotčená osoba právo na informaci o vhodných zárukách.

Právo na opravu

- Dotčená osoba má právo neprodleně požádat odpovědnou osobu o opravu nesprávných osobních údajů, které se jí týkají. S přihlédnutím k účelům zpracování má dotčená osoba právo požadovat doplnění neúplných osobních údajů — a to i prostřednictvím dodatečného prohlášení.

Právo na výmaz („právo na zapomenutí“):

- Dotčená osoba má právo požadovat, aby odpovědná osoba neprodleně vymazala její příslušné osobní údaje, a odpovědná osoba je povinna tyto osobní údaje neprodleně vymazat za předpokladu, že platí jeden z těchto důvodů:
    1. Osobní údaje již nejsou nezbytné pro účely, pro které byly pořízeny nebo jinak zpracovány;
    2. Dotčená osoba odvolá svůj souhlas, o který se zpracování podle článku 6 odstavec 1 písmeno a GDPR nebo podle článku 9 odstavec 2 písmeno a GDPR opírá, a pro zpracování chybí jiný právní základ;
    3. Dotčená osoba podá námitku podle článku 21 odstavec 1 GDPR proti zpracování a neexistují žádné přednostní oprávněné důvody pro zpracování, nebo dotčená osoba podá proti zpracování námitku podle čl. 21 odstavec 2 GDPR ;
    4. Osobní údaje byly zpracovány protiprávně;
    5. Výmaz osobních údajů je nezbytný ke splnění právní povinnosti podle práva členských států, kterým odpovědná osoba podléhá;
    6. Osobní údaje byly pořízeny v souvislosti s nabízenými službami informační společností v souladu s článkem 8 odstavec 1 GDPR.

Právo na omezení zpracování:

- Dotčená osoba má právo požadovat, aby odpovědná osoba omezila zpracování, je-li splněn jeden z následujících předpokladů:
- pokud dotčená osoba zpochybňuje přesnost osobních údajů a sice po dobu, která odpovědné osobě umožní ověřit správnost osobních údajů:
- pokud je zpracování protiprávní a dotčená osoba výmaz osobních údajů odmítá a místo toho požaduje omezení užívání osobních údajů;
- pokud odpovědná osoba osobní údaje pro účely zpracování dále nepotřebuje, ale dotčená osoba je přesto potřebuje k uplatnění, vykonání nebo obhajování právních nároků,
- pokud dotčená osoba vznesla námitky proti zpracování podle článku 21 odstavec 1, zatímco dosud není stanoveno, za oprávněné důvody odpovědné osoby převažují nad důvody dotčené osoby.

Dotčená osoba by měla být požádána, aby svou žádost předložila písemně, a to buď e-mailem, nebo poštou, příslušnému místnímu inspektorovi ochrany údajů. Místní inspektor ochrany údajů musí dotčené osobě neprodleně zpřístupnit informace, v každém případě však do jednoho měsíce od obdržení žádosti. Je-li to nezbytné, může být tato lhůta prodloužena o další dva měsíce s ohledem na složitost a počet žádostí. Koordinátor ochrany údajů nebo inspektor ochrany údajů informuje dotčenou osobu o prodloužení lhůty do jednoho měsíce od obdržení žádosti spolu s důvody zpoždění. Dotčené osobě nevznikají žádné náklady za vyžádání informací, které o něm koncernová společnost Arbonia vlastní, pokud nejsou žádosti dotčené osoby zjevně neopodstatněné nebo nepřiměřené, zejména v důsledku opakovaného stanoviska. Žádosti dotčené osoby většímu počtu koncernových společností Arbonia musí být předány Corporate IT z důvodu koordinace a za účelem odpovědi.

7.5 Provedení posouzení dopadů na ochranu údajů

Pokud může plánovaná nová forma zpracování osobních údajů, zejména v případě používání nových technologií, přinést vysoké riziko pro práva a svobody dotčené osoby, vzhledem k povaze, rozsahu, okolnostem a účelům zpracování, je třeba dopředu uskutečnit posouzení důsledků předpokládaných operací zpracování na ochranu osobních údajů.

Před implementací nových operací zpracování je proto třeba posoudit z toho vyplývající rizika pro osobnost a základní práva dotčené osoby. U nových IT aplikací to musí být zohledněno v rámci procesu schvalování. Pokud se na základě prvotního posouzení vyvodí závěr, že plánovaná nová forma zpracování osobních údajů povede pravděpodobně k vysokému riziku pro dotčené osoby, je třeba provést posouzení dopadu na ochranu údajů.

Žádosti týkající se nutnosti, resp. během provádění posouzení dopadů na ochranu údajů by měly být adresovány místnímu koordinátorovi ochrany údajů nebo místnímu inspektorovi ochrany údajů. Po provedení je třeba posouzení dopadů na ochranu údajů oznámit místnímu koordinátorovi ochrany údajů nebo místnímu inspektorovi ochrany údajů a vyžádat si jeho stanovisko.

Pokud z posouzení dopadů na ochranu údajů vyplývá, že by zpracování vedlo k vysokému riziku pro dotčenou osobu a že nejsou přijata žádná opatření ke zmírnění rizika, je třeba před provedením nových operací zpracování konzultovat orgán dozoru.

8 BEZPEČNOST OSOBNÍCH ÚDAJŮ

Osobní údaje musí být chráněny před nezákonným přístupem a nezákonným zpracováním nebo zveřejněním, jakož i před neúmyslnou ztrátou, změnou nebo zničením. To platí bez ohledu na to, zda jsou osobní údaje zpracovávány elektronicky nebo v papírové podobě.

Odpovědné osoby a zpracovatelé objednávky musí realizovat vhodná technická a organizační opatření na ochranu údajů před nezákonným zpracováním. Tato opatření musí být založena na (i) osvědčených postupech, (ii) rizicích zpracování a (iii) potřebě chránit osobní údaje (stanovené postupem pro klasifikaci informací); obsahují mj. dle potřeby:

(a) pseudonymizace a šifrování osobních údajů;

(b) schopnost zajistit po dlouhou dobu důvěrnost, integritu, dostupnost a odolnost systémů a služeb souvisejících se zpracováním;

(c) schopnost rychle obnovit dostupnost osobních údajů a přístup k nim v případě fyzického nebo technického incidentu;

(d) postup pravidelného kontrolování, hodnocení a evaluace účinnosti technických a organizačních opatření k zajištění bezpečnosti zpracování.

Technická a organizační opatření na ochranu osobních údajů jsou součástí vnitřního řízení bezpečnosti informací a musí se neustále přizpůsobovat technickému vývoji a organizačním změnám.

Bezpečnostní postupy mohou minimálně zahrnovat následující:

- kontroly přístupu: Každý cizí subjekt nalezený v oblastech s kontrolou přístupu by měl být nahlášen.

- bezpečné uzamykatelné zásuvky nebo kartotéky: Pracovní stůl a skříňky by měly zůstat zamčené, pokud obsahují důvěrné informace jakéhokoli druhu. Osobní údaje jsou vždy důvěrné informace. Zaměstnanci by měli zajistit, aby papír a výtisky obsahující osobní údaje nebyly obecně na očích, například v tiskárně. Pokud jsou osobní údaje uloženy s oprávněním na datovém nosiči (například CD, USB, či DVD), je třeba tyto bezpečně ukládat, pokud nejsou používány.

- Způsoby likvidace: Papírové dokumenty by měly být skartovány a bezpečně zlikvidovány, pokud již nejsou zapotřebí. To platí i pro osobní údaje, které jsou obvykle uloženy elektronicky, avšak které byly vytištěny.

- údaje uložené v elektronické podobě: Osobní údaje by měly být odpovídajícím způsobem chráněny hesly v souladu s aktuálními směrnicemi pro hesla a nikdy by neměly být sdíleny mezi zaměstnanci. Je-li vhodná elektronická podoba, musí být osobní údaje uloženy a načteny v systémech IT serverů a ve strukturovaných aplikacích informačních technologií, nikoli v nešifrované podobě na místních počítačích.

- Osobní údaje shromážděné v elektronické podobě poskytnuté dotčenou osobou: totožnost dotčené osoby musí být ověřena, nejlépe dvojitým opt-in procesem (tj. druhým e-mailem k validaci uvedené e-mailové adresy). Pokud je přístup k webové stránce nebo aplikaci omezen na registrované uživatele (tj. uživatelský účet), musí identifikace a ověření dotčené osoby poskytovat bezpečnostní ochranu, která je úměrná příslušnému obsahu během přístupu.

- Uplatňování obezřetnosti při sdílení osobních údajů: Osobní údaje by nikdy neměly být neformálně sdíleny. Platí zásada "potřebných informací". Je zde povinný koncept členění a oddělení podle obchodní transakce, jakož i realizace rolí a odpovědností. Osobní údaje musí být před předáváním v elektronické podobě zašifrovány. Manažer informačních technologií může vysvětlit, jakým způsobem se osobní údaje zasílají autorizovaným externím kontaktním osobám.

- Vyžádat si instrukce: V případě otázek nebo nejistoty týkajících se aspektu ochrany údajů nebo povinností vyplývajících z této směrnice o ochraně údajů je třeba požádat o radu přímého nadřízeného, příslušného místního inspektora ochrany údajů nebo Legal & Compliance.

GDPR vyžaduje, aby bylo soukromí zohledněno co možná nejdříve. Soukromí prostřednictvím záměrné a standardní ochrany vyžaduje, aby organizace soukromí zvážily v prvních fázích záměrné a standardní ochrany a při celkovém průběhu vývoje nových produktů, procesů nebo služeb souvisejících se zpracováním osobních údajů. Soukromí ve výchozím nastavení znamená, že pokud systém nebo služba zahrnuje rozhodnutí jednotlivce o tom, kolik osobních údajů sdílí s ostatními, výchozí nastavení by měla být takového druhu, aby poskytovala největší ochranu soukromí. Proto každá nová IT aplikace podléhá internímu schvalovacímu procesu, v jehož rámci musí být tato nová IT aplikace v rámci evaluace rovněž vyhodnocena z hlediska právních předpisů o ochraně údajů.

ARBONIA

9 HLÁŠENÍ INCIDENTŮ V OBLASTI BEZPEČNOSTI ÚDAJŮ

Mnoho platných předpisů o ochraně údajů vyžaduje přímé hlášení incidentů v oblasti ochrany údajů zákonodárci. Proto je nutné, aby všechny incidenty v oblasti zabezpečení údajů byly neprodleně oznámeny příslušnému koordinátorovi ochrany údajů nebo inspektorovi ochrany údajů bez ohledu na to, zda je ovlivněn místní systém nebo koncernový systém, v souladu s postupem popsaným v pokynu společnosti Arbonia k incidentům v oblasti bezpečnosti údajů („Arbonia Data Breach Policy"). Pokud IT zjistí incidenty nebo rizika v oblasti zabezpečení dat, musí být nahlášeny stejným způsobem jako pokyny k Data Breach Notification.

Cílem je splnit povinnost hlášení porušení platných povinností ochrany údajů podle platných zákonů o ochraně údajů (např. podle GDPR nejpozději do 72 hodin od obdržení informace).

V takovém případě musí být kladen důraz na dodržení příslušných termínů pro oznámení o narušení bezpečnosti údajů a přijetí okamžitých opatření k prošetření incidentů a určení, zda byly osobní údaje skutečně porušeny. Corporate IT musí vést interní seznam narušení bezpečnosti ve společnosti Arbonia, aby mohly být podle národních právních předpisů splněny povinnosti podávat hlášení a musí zajistit, aby se příslušná pravidla pro zastupování používala tak, aby bylo možné tato porušení kdykoliv nahlásit. Před nahlášením národnímu úřadu je třeba informovat Corporate IT, a oddělení Legal and Compliance koncernu.

Je třeba striktně dodržovat všechny ostatní pokyny Corporate IT a místních IT oddělení.

10 DŮSLEDKY V PŘÍPADĚ NEDODRŽOVÁNÍ

Dodržování těchto zásad ochrany údajů má pro společnost Arbonia a její veřejné vnímání prvořadý význam. Nevhodné zpracování osobních údajů nebo jiná porušení zákonů o ochraně osobních údajů může v mnoha zemích rovněž podléhat trestnímu právu a může vést k nárokům na náhradu škody. V rámci společnosti Arbonia může porušení pravidel těchto zásad ochrany údajů vést k sankcím podle zákona a/nebo příslušné (pracovní) smlouvy.

11 ODCHYLKY

Odchylky od ustanovení tohoto pokynu a dodatků jsou povoleny pouze po konzultaci s Head of Legal & Compliance.

12 INFORMACE

Informace v souvislosti s pokyny o ochraně údajů uděluje Head of Legal & Compliance.

ARBONIA

13 VSTOUPENÍ V PLATNOST

Tento pokyn vstupuje v platnost 17. června 2020 a nahrazuje pokyn o zacházení s údaji (Pokyn o ochraně údajů) z 5. prosince 2013.

V Arbonu, 16. června 2020

Arbonia AG

Alexander von Witzleben
prezident správní rady a CEO

Andrea Wickart
Head of Legal & Compliance / generální sekretářka

Dodatky k tomuto pokynu o ochraně údajů společnosti Arbonia

Následující dodatky v jejich aktuální verzi konkretizují tento návod o ochraně osobních údajů:

- Pokyny k žádostem dotčených osob a k vymazání údajů
- Pokyny k narušení bezpečnostních údajů
- Prohlášení o ochraně osobních údajů pro pracovníky

Tento dokument je platný bez podpisu.