

POLITIKA OCHRANY OSOBNÍCH ÚDAJŮ

1. Tato „**politika ochrany osobních údajů**“ (dále jen „**politika**“) představuje požadavky, pravidla a předpisy na ochranu osobních údajů platné ve společnosti BPH – British Publishing House LTD se sídlem Level 17, Dashwood House, 69 Old Broad Street, London, EC2M 1QS, Company Nr. 08659692, v souvislosti s platností Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob při zpracovávání osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (obecné nařízení o ochraně údajů) (Úřední věstník L 119, s. 1). Za aplikaci této směrnice je odpovědná společnost, organizační složka odpovědná za bezpečnost informací, organizační složky, které ve velkém rozsahu zpracovávají osobní údaje, jiné organizační složky, jakož i všichni zaměstnanci společnosti. Společnost se bude v přiměřeném rozsahu snažit zajistit, aby tuto politiku dodržovali i její smluvní partneři, pokud jim poskytuje osobní údaje.

2. Politika obsahuje:

- a) popis zásad ochrany osobních údajů platných ve společnosti;
- b) postupy a pokyny pro konkrétní oblasti při ochraně osobních údajů, které je třeba vyjasnit ve zvláštních dokumentech.

3. Směrnice byla přijata rozhodnutím vedení společnosti ze dne 25. 5. 2018. Vedení společnosti odpovídá za realizaci a aplikaci směrnice ve společnosti.

4. ZKRATKY A POJMY:

- a) „Ast“ je NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob při zpracovávání osobních údajů a o volném pohybu těchto údajů, kterým se ruší směrnice 95/46/ES (obecné nařízení o ochraně údajů) (Úřední věstník L 119, s 1).
- b) „Údaje“ jsou osobní údaje, pokud z kontextu nevyplývá něco jiného.
- c) „Citlivé údaje“ jsou specifické údaje a trestněprávní údaje.
- d) „Zvláštní údaje“ jsou údaje podle článku 9 odst. 1 ast, tedy údaje, které odhalují rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech a zpracovávání genetických údajů, biometrických údajů pro individuální identifikaci fyzické osoby, údajů týkajících se zdraví nebo údajů týkajících se sexuálního života nebo sexuální orientace fyzické osoby.
- e) „Trestněprávní údaje“ jsou údaje podle článku 10. ast, tedy údaje týkající se uznání viny za trestné činy a přestupky.
- f) „Údaje dětí“ jsou osobní údaje o dětech mladších 16 let.
- g) „Osoba“ je osoba, které se osobní údaje týkají, pokud z kontextu nevyplývá něco jiného.
- h) „Zprostředkovatel“ je organizace nebo osoba, kterou společnost pověřila zpracováním osobních údajů (např. Poskytovatel IT služeb externího účetnictví).

- i) „Profilování“ je jakékoli automatizované zpracování osobních údajů založené na tom, že se osobní údaje používají k vyhodnocování určitých osobních aspektů týkajících se fyzických osob, především na analyzování nebo prognózování takových aspektů, jakými jsou pracovní výkon, ekonomická situace, zdravotní stav, osobní preference, zájmy, spolehlivost, chování, místo pobytu nebo změna pobytu konkrétní fyzické osoby.
- j) „Export osobních údajů“ je přenos osobních údajů do třetích zemí nebo do mezinárodní organizace.
- k) „Odpovědná osoba“ – vztahuje se na osobu odpovědnou za ochranu osobních údajů.
- l) „Seznam“ je seznam zpracovatelských činností.

5. OCHRANA OSOBNÍCH ÚDAJŮ V RÁMCI SPOLEČNOSTI – OBECNÉ ZÁSADY

5.1 Základní zásady ochrany osobních údajů v rámci společnosti:

- a) Zásada zákonnosti – společnost zajišťuje ochranu soukromé sféry a zpracovává osobní údaje v souladu se zákonem.
- b) Zásada bezpečnosti – společnost zajišťuje přiměřenou bezpečnost osobních údajů a v této oblasti vyvíjí soustavnou činnost.
- c) Zásada zachování práv jednotlivce – společnost umožní osobám, jejichž osobní údaje zpracovává, aby uplatnily svá práva v souladu s ast a zajišťuje jejich realizaci.
- d) Zásada odpovědnosti – společnost dokumentuje způsob, jakým si plní povinnosti v souvislosti s ochranou osobních údajů, aby byla kdykoliv schopna prokázat dodržování ast.

5.2 Zásady zpracování osobních údajů v rámci společnosti

Společnost při zpracování osobních údajů dodržuje následující zásady:

- a) legitimní základ a soulad s právními předpisy (legalismus);
- b) spolehlivost a čestnost (spolehlivost);
- c) transparentnost pro dotčenou osobu (transparentnost);
- d) na konkrétní účely, a ne „do zásoby“ (minimalizace);
- e) ne více, než je třeba (přiměřenost);
- f) kvalita osobních údajů (správnost);
- g) ne déle, než je potřeba (časové omezení);
- h) zajištění přiměřené bezpečnosti dat (bezpečnost).

5.3 Systém ochrany osobních údajů

Systém ochrany osobních údajů v rámci společnosti sestává z následujících prvků:

1) Inventarizace dat. Společnost identifikuje zdroje osobních údajů ve společnosti, kategorie osobních údajů, vztahy mezi zdroji dat, identifikuje metody použití dat (inventář), a to konkrétně:

- a) případy zpracování zvláštních a „trestněprávních“ údajů (citlivé údaje);
- b) případy zpracování údajů osob, které společnost neidentifikuje (neidentifikované údaje);
- c) případy zpracování osobních údajů dětí;
- d) případy profilování;
- e) případy spoluúčasti na zpracování osobních údajů.

2) Seznam. Společnost sestaví, vede a provozuje seznam činností v souvislosti s osobními údaji ve společnosti (dále jen „seznam“). Seznam je nástrojem na dodržování předpisů o ochraně osobních údajů ve společnosti.

3) Legitimní základ. Společnost zajišťuje, identifikuje a ověřuje legitimní základ ochrany osobních údajů a:

- a) provozuje systém správy souhlasů se zpracováním osobních údajů,
- b) inventarizuje a detailizuje zdůvodnění v případech, kdy společnost zpracovává údaje na základě svého oprávněného zájmu.

4) Zajišťování výkonu práv jednotlivce. Společnost si plní informační povinnost vůči osobám, jejichž osobní údaje zpracovává, a zajišťuje výkon jejich práv realizací průzkumů, jako například:

- a) Informační povinnost. Společnost poskytuje osobám při shromažďování údajů a v jiných situacích v souladu s požadavky a právně relevantní informace a zabezpečuje dokumentaci realizace těchto povinností.
- b) Možnost podávat žádosti. Společnost zajišťuje efektivní realizaci jakýchkoliv přiměřených žádostí v souvislosti se sebou nebo se svými zpracovateli.
- c) Zpracování žádostí. Společnost vynakládá přiměřené výdaje a postupy pro zajištění toho, aby žádosti osob, jejichž údaje zpracovává v souladu s požadavky a lhůtami a, byly řádně a včas prokázány.
- d) Informování o porušení ochrany osobních údajů. Společnost používá postupy, které umožňují informovat osoby o zjištěném porušení ochrany osobních údajů.

5) Minimalizace. Společnost používá zásady a metody minimalizace (Privacy by Default), např.:

- a) zásada přiměřenosti při správě osobních údajů;
- b) zásada regulace a správy přístupu k osobním údajům;
- c) zásady časového managementu úschovy osobních údajů a ověřování jejich vhodnosti.

6) Bezpečnost. Společnost zajišťuje přiměřenou bezpečnost osobních údajů, např.:

- a) analyzuje rizika aktivit nebo kategorií při zpracování dat;
- b) posuzuje následky činností v souvislosti s ochranou osobních údajů, které mají vysoké riziko porušení práv a svobod osob;
- c) adaptuje opatření na ochranu osobních údajů na dohodnuté riziko;
- d) vlastní systém managementu informační bezpečnosti;
- e) používá postupy pro identifikaci, vyhodnocování a hlášení zjištěných porušení ochrany osobních údajů příslušnému orgánu na ochranu osobních údajů, který porušení spravuje.

7) Zprostředkovatelé. Společnost má vypracovaná pravidla pro výběr zprostředkovatelů, pravidla pro určování požadavků na zpracování (smlouvy o předávání údajů/pravidla zpracování apod.), pravidla kontroly realizace smluv o přenosu dat (kontroly/audity apod.).

8) Export osobních údajů. Společnost má vypracovaná pravidla pro kontrolu toho, aby neposkytla údaje třetím zemím (tj. mimo EU, Norsko, Lichtenštejnsko, Island) ani mezinárodním organizacím, resp. aby byly takové přenosy realizovány v souladu se zákonem.

9) Privacy by Design. Společnost spravuje změny v oblasti zpracování osobních údajů, které mají negativní vliv na ochranu osobních údajů. Z tohoto důvodu postupy pro implementaci nových projektů a investic zohledňují potřebu vyhodnocovat vlivy změn na ochranu osobních údajů a chránit soukromí již při tvorbě změn, investic nebo na začátku nového projektu (patří sem dodržování cílů zpracování údajů, bezpečnosti a minimalizace údajů).

10) Přeshraniční zpracování. Společnost má vypracovaná pravidla pro ověřování případů přeshraničního zpracování údajů, jakož i pravidla pro vytvoření kontrolního orgánu a hlavní organizační jednotky ve smyslu ast.

6. INVENTURA

6.1 Citlivé osobní údaje. Společnost identifikuje případy, kdy dochází nebo může docházet ke zpracování citlivých osobních údajů (zvláštní a trestněprávní údaje), a používá speciální mechanismy,

kteří umožňují zpracovat citlivé údaje v souladu se zákonem. V případě identifikace zpracování citlivých osobních údajů se společnost řídí schválenými pravidly.

6.2 Neidentifikované osobní údaje. Společnost identifikuje případy, kdy dochází nebo může docházet ke zpracování neidentifikovaných osobních údajů, a používá mechanismy, které usnadňují realizaci práv osob dotčených zpracováním neidentifikovaných údajů.

6.3 Profilování. Společnost identifikuje případy, kdy dochází k profilování zpracovávaných dat a používá mechanismy, které zajistí, že tento proces proběhne v souladu se zákonem. V případě identifikace profilování a automatizovaného rozhodování se společnost řídí příslušnými pravidly.

6.4 Spoluúčast na správě osobních údajů. Společnost identifikuje případy, kdy dochází k spoluúčasti na správě osobních údajů a postupuje ve smyslu přijatých pravidel.

7. SEZNAM ZPRACOVATELSKÝCH ČINNOSTÍ

7.1 Seznam zpracovatelských činností (ZSC) je formou dokumentace zpracovatelských činností, slouží jako mapa zpracování údajů a je jedním z klíčových prvků, které umožňují realizaci základní zásady, na níž je založen celý systém ochrany osobních údajů – zásady odpovědnosti.

7.2 Společnost vede seznam zpracovatelských činností, kontroluje a dohlíží na způsob používání osobních údajů.

7.3 Seznam je jedním ze základních nástrojů, které společnosti umožňují plnit většinu závazků vyplývajících z ochrany osobních údajů.

7.4 Pro každou činnost v souvislosti se zpracováním osobních údajů, kterou společnost pro účely seznamu zaznamenává zvlášť, v seznamu eviduje minimálně následující údaje: (i) činnost, (ii) účel zpracování, (iii) popis kategorie dotčené osoby, (iv) popis kategorie údajů, (v) popis kategorie příjemce dat (včetně zprostředkovatelů), (vi) informace o přenosu mimo EU/EHP, (vii) obecný popis technických a organizačních opatření na ochranu osobních údajů.

8. ZÁSADY ZPRACOVÁNÍ

8.1 Společnost si určuje legitimní základ pro zpracování osobních údajů pro konkrétní zpracovatelské činnosti.

8.2 Společnost si určuje obecné základy (souhlas, smlouva, povinnost ze zákona, zásadní zájem, oprávněný účel společnosti) v případě potřeby v čitelné formě. Například při souhlasu uvede rozsah, pokud je legitimním základem právní předpis – odkazem na konkrétní předpis a jiné dokumenty, např. smlouvu, životně důležité zájmy – uvedení kategorie událostí, při kterých nastávají při legitimním účelu – odkazem na konkrétní cíl, např. vlastní marketing, uplatnění nároků.

8.3 Společnost realizuje metody pro správu souhlasů, aby si zajistila přehled o registraci a ověřování souhlasů se zpracováním specifických údajů pro konkrétní účel, s komunikací přes telekomunikační prostředky (e-mail, telefon, SMS atd.), jakož i o odepřených souhlasech, odvolaných souhlasech a podobných činnostech (odvolání, omezení apod.).

8.4 Vedoucí organizační složky musí znát právní základ, na kterém organizační složka, kterou vede, vykonává činnosti v souvislosti se zpracováním osobních údajů. Pokud je základem oprávněný zájem společnosti, vedoucí musí znát specifické zájmy společnosti, které se zpracovávají.

9. ZPŮSOB OCHRANY JEDNOTLIVCE A INFORMAČNÍ POVINNOST

9.1 Podnik dbá na čitelnost a styl poskytnuté informace a komunikace s osobami, jejichž osobní údaje zpracovává.

9.2 Společnost odpovídá za čitelnost a styl poskytnuté informace a komunikace s osobami, jejichž osobní údaje zpracovává.

9.3 Společnost usnadňuje osobám, jejichž údaje zpracovává, výkon jejich práv různými aktivitami, jako například: zveřejňování informací nebo linků o jejich právech na internetových stránkách společnosti, způsob jejich užívání ve společnosti, mimo jiné požadavky na identifikaci, možnosti navázání kontaktu se společností za tímto účelem, případný ceník „dodatečných“ žádostí apod.

9.4 Společnost dbá na dodržování zákonných lhůt a na plnění závazků vůči osobám, jejichž osobní údaje zpracovává.

9.5 Společnost zavádí přiměřené metody pro identifikaci a autentizaci osob, jejichž osobní údaje zpracovává, aby mohla realizovat individuální práva jednotlivce a zajišťovat informační povinnost vůči jednotlivcům.

9.6 Za účelem výkonu práv společnosti společnost zajišťuje postupy a mechanismy, kterými údaje konkrétních osob identifikuje, integruje je, realizuje v nich změny a zajišťuje jejich výmaz.

9.7 Společnost dokumentuje plnění informačních povinností, poskytování informací a žádosti osob, jejichž osobní údaje zpracovává.

10. INFORMAČNÍ POVINNOST

10.1 Společnost efektivně a v souladu se zákonem definuje prostředky k plnění informačních povinností.

10.2 Společnost informuje osobu, jejíž údaje zpracovává, jestliže se lhůta pro posouzení její žádosti prodlouží na více než jeden měsíc.

10.3 Společnost informuje osobu, jejíž osobní údaje získává, že tyto budou zpracovány.

10.4 Společnost informuje osobu, jejíž údaje získává nepřímo, že tyto budou zpracovány:

- a) v přiměřené lhůtě po získání osobních údajů – nejpozději do jednoho měsíce – při zohlednění specifických okolností zpracování osobních údajů;
- b) jestliže osobní údaje mají být použity pro komunikaci s dotyčnou osobou – nejpozději při první komunikaci s dotyčnou osobou; nebo
- c) pokud je plánováno poskytnutí osobních údajů jinému příjemci – nejpozději při prvním zveřejnění.

10.5 Tam, kde je to možné, společnost definuje způsob, jakým osoby informuje o zpracování neidentifikovaných údajů (např. upozornění o nahrávání kamerového záznamu).

10.6 Společnost informuje osoby, jejichž údaje zpracovává, o plánované změně účelu zpracování údajů.

10.7 Podnik informuje osoby, jejichž údaje zpracovává, o zrušení omezení při zpracování.

10.8 Společnost informuje příjemce údajů o opravě, výmazu nebo omezení při zpracování údajů (pokud to není spojeno s nepřiměřenými náklady, resp. nemožné).

10.9 Společnost informuje osoby, jejichž údaje zpracovává, nejpozději při prvním kontaktu o tom, že jsou oprávněny podat námitky proti zpracování svých osobních údajů.

10.10 Pokud hrozí vysoké riziko porušení práv nebo svobod osoby, společnost osobu neprodleně informuje o každém porušení ochrany jejích osobních údajů.

11. ŽÁDOSTI OSOB, jejichž údaje jsou zpracovávány

11.1 Práva třetích osob. Realizací práv osob, jejichž údaje zpracovává, společnost zavádí garance na ochranu práv a svobod třetích osob. Zejména pokud má spolehlivé informace, že splněním žádosti osoby, aby vydala kopii dat nebo právem na přenos dat, by mohla být dotčena práva a svobody jiných osob (např. práva, která jsou spojena s ochranou údajů jiných osob, práva duševního vlastnictví, obchodní tajemství, osobní práva apod.), může společnost požádat osobu, která žádost podala, aby vysvětlila pochybnosti nebo může podniknout jiné zákonné kroky až po odmítnutí splnění žádosti.

11.2 Nezpracování údajů. Společnost na požádání poskytne osobě informaci, že nezpracovává její osobní údaje.

11.3 Odmítnutí. Společnost na požádání do jednoho měsíce po obdržení žádosti informuje dotyčnou osobu, že odmítá její žádost splnit, a zároveň ji informuje o právech a povinnostech, které jsou s tím spojené.

11.4 Přístup k údajům. Na požádání osoby v souvislosti s přístupem k jejím údajům společnost osobě oznámí, zda její osobní údaje zpracovává, a informuje ji o podrobnostech zpracování v souladu s čl. 15 ast (rozsah odpovídá informační povinnosti při získávání dat) a osobě, která o to požádá, poskytne přístup k těmto údajům. Přístup k údajům může být poskytnut předáním kopie dat s upozorněním, že každá další kopie dat může být zpoplatněna.

11.5 Kopie údajů. Společnost na požádání vydá dotyčné osobě kopii jejích údajů a předání první kopie zaeviduje. Společnost má ceník kopií údajů, podle kterého vyměřuje poplatky za další kopie. Cena za kopii údajů se vypočítá na základě odhadovaných nákladů na zpracování žádosti o vydání kopie dat.

11.6 Nezpracování údajů. Společnost na požádání informuje osobu, že její osobní údaje nezpracovává.

11.7 Oprava osobních údajů. Společnost na základě odůvodněné žádosti dotyčného opraví nesprávné osobní údaje. Společnost je oprávněna odmítnout opravu osobních údajů, pokud dotyčná osoba neprokáže nesprávnost údajů, jejichž opravu žádá. Pokud je to možné a pokud to není spojeno s nepřiměřenými náklady, společnost informuje každého příjemce, kterému poskytla osobní údaje, že tyto byly opraveny. Pokud to osoba, která je opravenými údaji dotčena, požaduje, společnost ji o těchto příjemcích informuje.

11.8 Doplnění údajů. Společnost na žádost dotyčné osoby doplňuje a aktualizuje osobní údaje. Společnost je oprávněna odmítnout doplnění údajů v případě, že je to neslučitelné s cíli zpracování dat (např. pokud společnost údaje požadované dotyčnou osobou na zpracování nepotřebuje). Společnost se na prohlášení dotyčné osoby v souvislosti s doplňujícími údaji může spolehnout, pokud to neznemožňují postupy, které společnost používá (např. při získávání dat), zákonné předpisy nebo pokud nastanou důvody, pro které je takové doplňkové prohlášení nedůvěryhodné.

11.9 Vymazání údajů. Společnost na žádost dotyčné osoby údaje vymaže, pokud:

- a) údaje pro účely, pro které byly získány nebo zpracovány, nejsou potřeba;
- b) byl odvolán souhlas ke zpracování a neexistuje jiný legitimní základ pro jejich zpracování;
- c) dotyčná osoba podala účinnou námitku proti zpracování údajů;
- d) údaje byly zpracovány v rozporu se zákonem;
- e) pokud potřeba údaje vymazat vyplývá ze zákonné povinnosti;
- f) se žádost týká údajů dítěte, které se uchovávají na základě souhlasu s poskytnutím služby informační společnosti (např. profil dítěte v sociální síti, účast v soutěži na internetové stránce).

Společnost určí, jak se právo na vymazání osobních údajů realizuje, aby byla zajištěna efektivní realizace tohoto práva v souladu se zásadami ochrany osobních údajů a aby nedocházelo k výjimkám v souladu s čl. 17. odst. 3 ast. Pokud společnost zveřejnila osobní údaje, které je povinna vymazat, podnikne přiměřená, mimo jiné i technická opatření, aby informovala jiné zprostředkovatele, kteří dotyčné údaje zpracovávají, o povinnosti vymazat je.

V případě vymazání osobních údajů společnost na požádání informuje dotyčnou osobu o příjemcích údajů.

11.10 Omezení zpracování. Společnost zpracování dat na žádost dotyčné osoby omezí, jestliže:

- a) Zpracování je v rozporu se zákonem a dotyčná osoba nesouhlasí s vymazáním osobních údajů a namísto toho požaduje omezení jejich zpracování;
- b) Osobní údaje nepotřebuje společnost, ale na zjištění, uplatnění nebo obhajobu svých nároků je potřebuje dotyčná osoba.
- c) Dotyčná osoba odmítla zpracování z důvodů souvisejících s její specifickou situací, dokud se nezjistí, zda společnost nemá právní nadřazené oprávněné nároky na zpracování.

Během omezení zpracování společnost údaje uchovává, ale bez souhlasu dotyčné osoby je nezpracovává (nepoužívá je ani je neposkytuje dále), pokud není třeba zjistit nebo chránit práva jiné fyzické či právnické osoby nebo pokud tomu neodporují významné důvody veřejného zájmu.

Podnik informuje osobu o zrušení omezení zpracování.

V případě omezení zpracování osobních údajů společnost na požádání informuje osobu o příjemcích údajů.

11.11 Přenos dat. Společnost na požádání poskytne osobě, jejíž údaje jsou zpracovávány, tyto údaje ve strukturovaném, běžně používaném formátu, který je čitelný na počítači, nebo je poskytne jinému podniku, pokud je to možné, v IT systému společnosti na základě souhlasu této osoby nebo za účelem uzavření nebo splnění uzavřené smlouvy.

11.12 Námitka ve specifické situaci. Jestliže osoba podá námitky proti zpracování osobních údajů, kterou odůvodňuje její specifická situace, a společnost tyto údaje zpracovává na základě oprávněného zájmu nebo při plnění úkolů veřejné služby, společnost k námitce přihlédne, kromě případů, kdy společnost k tomu nemá právně odůvodněný důvod, který by byl nadřazený zájmům, právům a svobodám osoby, která námitky podala, nebo který slouží jako základ pro zjištění, uplatnění nebo obranu nároků.

11.13 Vědecké, historické nebo statistické účely. Pokud společnost realizuje vědecký výzkum, historický výzkum nebo zpracovává údaje pro statistické účely, může osoba podat námitku, která je motivována její specifickou situací. Společnost k této námitce přihlédne, kromě případů, kdy je zpracování nezbytné pro splnění úkolu ve veřejném zájmu.

11.14 Námitka proti přímému marketingu. Pokud má osoba námitky proti zpracování svých údajů společností pro účely přímého marketingu (mj. např. na profilování), společnost k její námitce přihlédne a zpracování zastaví.

11.15 Právo na lidský zásah při automatizovaném zpracování. Pokud společnost automatizovaně zpracovává osobní údaje, především pokud profiluje osoby a následně ve vztahu k nim přijímá rozhodnutí, která mají pro osobu právní nebo jiné závažné důsledky, společnost nabízí možnost lidského zásahu do takového automatizovaného rozhodování, kromě případů, kdy je takové automatizované rozhodnutí (i) potřebné k uzavření nebo splnění smlouvy mezi subjektem údajů a společností, nebo (ii) je zákonem výslovně dovoleno, nebo (iii) se realizuje na základě výslovně uděleného souhlasu dotčené osoby.

12. MINIMALIZACE

Společnost zajišťuje minimalizaci zpracování osobních údajů s ohledem na: (i) přiměřenost údajů pro konkrétní účel (objem dat a rozsah zpracování), (ii) přístup k údajům, (iii) dobu archivování dat.

12.1 Minimalizace rozsahu. Společnost verifikuje rozsah získaných údajů, rozsah jejich zpracování a objem zpracovaných údajů vzhledem k jejich vhodnosti v rámci realizace ast. Společnost minimálně jednou za rok přezkoumá objem zpracovávaných dat a rozsah jejich zpracování. Společnost přezkoumá změny v objemu a rozsahu zpracovávání v rámci managementu změn („Privacy by Design“).

12.2 Minimalizace přístupu. Společnost používá omezení přístupu k osobním údajům: právní (povinnost zachovávat tajemství, schvalovací limity), fyzické (oblasti přístupu, uzavřené prostory) a logické (omezení práv k systémům, které zpracovávají osobní údaje, a síťové zdroje, ve kterých se nacházejí osobní údaje). Společnost provádí fyzické kontroly přístupu. Společnost aktualizuje přístupová práva ke změnám ve složení zaměstnanců a ke změnám úkolů osob, jakož i ke změnám ve zpracovatelských jednotkách. Společnost pravidelně kontroluje pověřené uživatele systému a nejméně jednou za rok aktualizuje. Podrobná pravidla fyzických a logických kontrol přístupu jsou obsažena v postupech technických organizačních opatření k zajištění ochrany zpracovávaných údajů, která byla přijata v rámci realizace směrnice.

12.3 Časová minimalizace. Společnost implementuje kontrolní mechanismy životního cyklu dat ve společnosti, jako například kontrolu další vhodnosti údajů na údaje a kontrolní body uvedené v seznamu. Údaje, jejichž rozsah použití je časově omezený, je třeba odstranit z výrobních systémů společnosti, jakož i z příručních spisů a hlavních databází. Tyto údaje je možné archivovat, nahrát na backup-systémy a zpracovat. Postupy na archivaci a používání archivů, vytváření a používání zabezpečovacích kopií zohledňují požadavky kontroly životního cyklu dat, včetně požadavku na jejich vymazání.

13. BEZPEČNOST

Společnost zajišťuje míru bezpečnosti osobních údajů odpovídající riziku porušení práv a svobod fyzických osob, ke kterému může dojít zpracováním osobních údajů společností.

13.1 Analýza rizik a přiměřenosti bezpečnostních opatření. Společnost provádí a dokumentuje analýzu přiměřenosti opatření k zajištění bezpečnosti osobních údajů. Za tímto účelem:

a) Společnost zajišťuje přiměřený stav poznatků o informační bezpečnosti, kyberbezpečnosti a kontinuitě činnosti, a to buď interně, nebo s podporou specializovaných zařízení.

b) Společnost kategorizuje údaje a zpracovatelské činnosti vzhledem k riziku, které představují.

c) Společnost analyzuje rizika porušení práv a svobod osob pro zpracovatelské činnosti a kategorie údajů. Společnost analyzuje možné situace a scénáře porušení osobních údajů při zohlednění typu, rozsahu, kontextu a účelu zpracování, rizika porušení práv a svobod osob s různou pravděpodobností vzniku a závažnosti rizika.

d) Společnost stanoví organizačně technická bezpečnostní opatření, která se dají použít, a vyhodnocuje náklady na jejich realizaci. Společnost určí vhodnost těchto opatření a při jejich realizaci aplikuje následující postupy:

(i) pseudonymizace,

(ii) šifrování osobních údajů,

(iii) jiná kyberbezpečnostní opatření sestávající ze schopnosti zajišťovat důvěryhodnost, integritu, dostupnost a odolnost zpracovatelských systémů a služeb,

(iv) opatření k zajištění kontinuity činnosti a předcházení katastrofám, tj. schopnost v případě fyzického nebo technického incidentu rychle obnovit přístupnost a přístup k osobním údajům.

13.2 Odhadování následků pro ochranu osobních údajů. Společnost vyhodnocuje následky plánovaných operací v souvislosti s ochranou osobních údajů, pokud na základě analýzy hrozí vysoké riziko porušení práv a svobod. Společnost aplikuje interní metody hodnocení následků.

13.3 Bezpečnostní opatření. Společnost aplikuje bezpečnostní opatření, která přijala na základě analýzy rizik a přiměřenosti bezpečnostních opatření a odhadu následků pro ochranu osobních údajů. Osobní opatření na ochranu údajů tvoří součást opatření informační bezpečnosti a kyberbezpečnosti v podniku a jsou podrobně popsána v postupech, které společnost pro tyto oblasti aplikuje.

13.4 Hlášení incidentů. Společnost aplikuje takové postupy, které umožňují identifikovat, vyhodnotit a odeslat příslušnému orgánu porušení ochrany údajů do 72 hodin od jeho zjištění.

14. ZPROSTŘEDKOVATEL

Společnost disponuje zásadami výběru a verifikace zpracování dat, aby bylo možné zajistit, že zpracovatelé poskytují společnosti dostatečné garance na realizaci přiměřených organizačně technických opatření k zajištění bezpečnosti, realizace individuálních práv a jiných závazků v souvislosti s ochranou osobních údajů. Společnost uzavírá smlouvy na zpracování osobních údajů splňující požadavky podle ast. Společnost zúčtovává zprostředkovatele jako subdodavatele, a to i v souvislosti s jinými požadavky vyplývajícími se zásad přenosu osobních údajů.

15. EXPORT DAT

Společnost eviduje v seznamu případy exportu dat, tedy jejich přenos v rámci Evropského hospodářského prostoru (EHP 2017 = Evropská unie, Island, Lichtenštejnsko a Norsko). Společnost za účelem zamezení neoprávněného exportu údajů, zejména v souvislosti s využíváním veřejně dostupných cloudových služeb (Shadow IT) pravidelně ověřuje chování uživatelů a podle možnosti jim poskytuje rovnocenné řešení na ochranu osobních údajů.

16. VYTVOŘENÍ SOUKROMÍ

Společnost spravuje změny týkající se ochrany osobních údajů tak, aby byla zajištěna přiměřená bezpečnost osobních údajů a aby bylo minimalizováno jejich zpracování. Z tohoto důvodu se zásady projektového a

investičního managementu vztahují na zásady ochrany osobních údajů a na minimalizaci jejich zpracování, což si od začátku projektu nebo investice vyžaduje zvažování následků pro ochranu soukromí a osobních údajů, zohledňování a vytváření bezpečnosti a minimalizaci zpracování osobních údajů.

17. ZÁVĚREČNÁ USTANOVENÍ

Ustanovení politiky mohou v rámci rozhodování vedení společnosti podléhat změnám.

Politika nabývá účinnosti 28. května 2018

BPH - BRITISH PUBLISHING HOUSE LTD
Level 17, Dashwood House
69 Old Broad Street
London, EC2M 1QS
Phone: +44 20 81 33 44 88
Email: office@britishpedia.com