ARCDATA PRAHA

esri Official Distributor

Podmínky zabezpečení, diskrétnosti a oznamování bezpečnostních incidentů

Článek I.
Prohlášení

1. Poskytovatel se zavázal příjemci poskytnout dohodnutou službu či dodat dohodnuté zboží.

2. Předmětem poskytované služby není žádná zpracovatelská operace ze strany poskytovatele ve vztahu ke příjemcem zpracovávaným osobním údajům. Byť není vyloučeno, že poskytovatel přijde při své činnosti pro příjemce do kontaktu s osobními údaji, informacemi o parametrech zpracování osobních údajů, včetně informací o zabezpečení, není oprávněn s nimi jakkoli disponovat.

3. Tyto podmínky jsou součástí smlouvy podle odst. 1. Stanoví-li smlouva něco jiného než tyto podmínky, má smlouva přednost.

Článek II.
Vymezení pojmů

1. Není-li výslovně stanoveno jinak, mají pojmy vymezené v čl. 4 obecného nařízení o ochraně osobních údajů shodný význam, který jim je přisouzen odkazovaným ustanovením obecného nařízení.

2. Dále se pro účely této smlouvy rozumí:

a. **bezpečnostním incidentem** – porušení zabezpečení osobních údajů, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů, nebo alespoň ohrožení náhodným nebo protiprávním zničením, ztrátou, změnou nebo neoprávněným poskytnutím nebo zpřístupněným osobních údajů, dále například i ztráta nebo neoprávněné zpřístupnění hesla, příp. přístupových údajů či prostředků do prostor zpracování osobních údajů, k uloženým či zpracovávaným osobním údajům, do multimediálních prostředků a prostředků výpočetní techniky určených ke zpracování osobních údajů nebo k jejich uložení; uvedené platí obdobně i pro informace o zabezpečení zpracování osobních údajů;

b. **oznamovatel** – člověk oznamující bezpečnostní incident;
c. **oznamovaný** – člověk, který není oznamovatelem a dotýká se jej bezpečnostní incident ve smyslu, že je původcem nebo zavdal příčinu k bezpečnostnímu incidentu.

Článek III.
Bezpečnostní opatření

1. Poskytovatel není oprávněn při své činnosti pro příjemce jakkoli aktivně přistupovat k osobním údajům zpracovávaným příjemcem, stejně tak jako k informacím o zpracování osobních údajů realizovaných příjemcem a ani k informacím o zabezpečení zpracování osobních údajů.
2. Přijde-li poskytovatel při činnosti pro příjemce v kontakt s osobními údaji, s informacemi o jejich zabezpečení, či s informacemi o parametrech zpracování osobních údajů, bude o nich zachovávat mlčenlivost. Povinnost mlčenlivosti v potřebné míře zajistí i u svých zaměstnanců a u dalších pro něj činných osob.
3. Při činnosti pro příjemce bude poskytovatel zachovávat maximální šetrnost při nakládání s nosiči informací a údajů ve smyslu odst. 1. Příjemce nebude do nosičů jakkoli zasahovat, zejména jde-li o zásahy, který by mohly vést k neoprávněnému zpřístupnění, změně, zničení, znepřístupnění, výmazu nebo předání takových informací nebo údajů. Uvedené platí přiměřeně i ve vztahu k opatřením a prostředkům určeným k zabezpečení takových údajů a informací.
4. Ve vztahu k naplnění účelu podle odst. 1 až 3 tohoto článku přijme poskytovatel potřebná bezpečnostní a technicko-organizační opatření.
5. Součástí řádného zabezpečení a plnění povinností podle odst. 1 až 4 je i pravidelné prověřování efektivity a dostatečnosti přijatých bezpečnostních opatření, školení zaměstnanců a osob zapojených do činnosti pro příjemce a ověřování jejich znalostí, správného chápání fungování bezpečnostních pravidel a dodržování stanovených opatření a postupů.

Článek IV.
Další opatření k zabezpečení

1. Bezpečnostní opatření poskytovatel provede na základě řádného zhodnocení rizik, jejich pravděpodobnosti a možných negativních důsledků z nich plynoucích pro práva a svobody dotčených osob. Primárním cílem musí být eliminovat rizika, tam kde to není možné pak rizika minimalizovat, a kde není ani to možné, eliminovat nebo alespoň minimalizovat možné negativní důsledky pro práva a svobody dotčených osob.
2. Poskytovatel krom jiného zavede a bude garantovat mj. tato pravidla a principy určené k zajištění bezpečnosti:
a. povinnost počínat si tak, aby nedošlo ke ztrátě, zničení či neoprávněné změně anebo zpřístupnění údajů a informací podle čl. III. odst. 1 a 2. V případě, že bezprostředně hrozí nebezpečí ztráty, neoprávněného zničení, změny či zpřístupnění takových informací nebo jejich nosičů, povinnost v nezbytném rozsahu přiměřeným způsobem zakročit. O provedeném zákroku, jeho důvodech, průběhu a důsledcích bez zbytečného odkladu informovat příjemce;
b. každý je povinen obratem zprávou elektronické pošty nebo písemně zpravit určenou odpovědnou osobu o každé závadě v podmínkách či jednotlivých parametrech zpracování, resp. zabezpečení;
c. zajistí se i další vhodná a potřebná bezpečnostní opatření, například pravidelnou vynucenou změnu přístupových hesel;
d. v maximální možné míře využívat technických a jiných možností zabezpečení, kterými jsou opatřeny pracovní a jiné prostředky, kterých se využívá při činnosti pro příjemce, zejména se zajistí povinnost zaměstnanců:
   i. uzamykání místností, skříní a jiných prostor, v nichž jsou uloženy nosiče osobních údajů, není-li v prostorech přítomen nikdo oprávněný přistoupit k předmětným osobním údajům a jejich nosičům;
   ii. při skončení práce s technickým či multimediálním zařízením anebo aplikacemi odhlášení z tohoto zařízení, prostředí či aplikace;
   iii. důsledné utajování hesel a přihlašovacích kódů pro přístup do zařízení, multimediálního prostředí či do jednotlivých aplikací;
   iv. volit bezpečná hesla, tj. hesla sestávající se nejméně z 8 alfanumerických i nealfanumerických znaků, kdy každé heslo musí obsahovat velká i malá písmena;
   v. v případě mobilních telefonů a jiných obdobných zařízení vždy zvolit zabezpečení pro spuštění a přihlášení do zařízení, stejně jako pro jeho odemčení, alespoň prostřednictvím zadáním čtyřmístného PIN; je-li to možné, zvolí se vždy i vyšší způsob zabezpečení;
   vi. na multimediální zařízení a výpočetní techniku, která byla zaměstnanci svěřena k plnění pracovních úkolů, bez svolení a asistence odpovědné osoby neinstalovat jakýkoli software, či neprovádět jakékoli změny, zejména pak vyřazovat antivirové a či jiné obdobné programy určené k zajištění bezpečnosti zpracovávaných osobních údajů;

vii. je-li zaměstnanci svěřen mobilní telefon nebo služební PC, či jiné obdobné multimediální zařízení či zařízení výpočetní techniky, zejména má-li zaměstnanec možnost disponovat s ním i mimo prostory zaměstnavatele, aby dotyčný přijal a důsledně provedl taková opatření, aby zcela vyloučil přístup a dispozice s těmito prostředky ze strany jakékoli třetí osoby, stejně tak jako opatření k tomu, aby předešel zničení či poškození takových zařízení.

Článek V.
Komunikace

1. Komunikace (telefonem, elektronickou poštou, běžnou poštou) související s činností poskytovatele pro příjemce, ať již je činěna v rámci jedné ze stran nebo mezi nimi či vůči třetím osobám (smluvním partnerům, klientům, státním úřadům atd.), se realizuje vždy maximálně bezpečně a diskrétně, tj. tak, aby se s obsahem zprávy, včetně předávaných informací a údajů, neměl možnost seznámit nikdo jiný než její oprávněný adresát.

2. K předávání zpráv obsahující informace podle čl. III. odst. 1 a 2 slouží: datová schránka, zpráva el. pošty, úložní el. služby, nebo doručování prostřednictvím poskytovatele poštovních služeb, příp. jiný obdobný způsob doručování, kdy dochází k fyzickému předání nosiče osobních údajů adresátovi (služby messengera atp.).

3. Je-li to s ohledem na povahu adresáta a poskytované služby možné, použije se ke komunikaci přednostně systém datových schránek.

4. Není-li možné k předání údajů využít systému datových schránek, lze využít, žádá-li si to to povaha předávaných informací a jejich zabezpečení, el. poštu nebo poskytovatele poštovních služeb, příp. jinou obdobnou službu, kdy dochází k fyzickému předání nosiče údajů (služba messengera atp.). V těchto případech je třeba vždy určit konkrétního adresáta a využít služby potvrzení doručení, resp. doručení do vlastních rukou.

5. Předání informací prostřednictvím zprávy el. pošty je v případech podle odst. 4 možné jedině při řádném zabezpečení předávaných informací. Zabezpečením se míní nejméně komprimace předávaného souboru do formátu *.zip nebo podobného formátu a kódování předmětného souboru prostřednictvím bezpečného hesla. Bezpečným heslem se míní heslo nejméně o 8 znacích, které obsahuje alfanumerické (velká i malá písmena a číslice) i nealfanumerické znaky. Heslo musí být s adresátem dohodnuto předem. Heslo musí být bezpečně předáno – bezpečným předáním není předání hesla v otevřené zprávě el. pošty; stejné platí o pro změnu hesla.

6. Dohodnuté heslo si diskrétně sdělí odpovědní zástupci smluvních stran.

Článek VI.
Bezpečnostní incident

1. Dozví-li se poskytovatel o bezpečnostním incidentu, je povinen jej bezodkladně oznámit příjemci. Stejné platí i o důvodném podezření na bezpečnostní incident.

2. Předpokladem oznámení ve smyslu tohoto článku je vždy:

a) poctivost na straně oznamovatele;

b) přesvědčení oznamovatele o pravdivosti oznámení;

c) přesvědčení oznamovatele o legálnosti jednání/oznámení;

d) ověření oznamovaných informací.

Jiná oznámení (neověřená, nepoctivá – vedená úmyslem někoho poškodit) mohou zakládat povinnosti nahradit újmu (hmotnou nebo nehmotnou).

3. Bezpečnostní incident se diskrétně oznamuje příjemce určené osobě.

4. Poskytovatel zajistí, aby oznamovatel vždy oznamoval tak, dotýká-li se oznámení některého se spoluzaměstnanců nebo členů poskytovatele nebo jiné osoby, kdy taková osoba má mít postavení porušitele právních povinností, aby se o oznámení nedozvěděl oznamovaný.

5. Oznámení se podává písemně nebo prostřednictvím zprávy el. pošty.

6. V oznámení se uvede (bude-li to z povahy věci možné):

a. jméno a příjmení, pracovní zařazení a kontaktní údaje oznamovatele;

b. vše, co o oznamovaném bezpečnostním incidentu oznamovatel a třetí osoby ví (popis bezpečnostního incidentu);

c. jména a příjmení všech osob, které se bezpečnostního incidentu účastnili, včetně jejich pracovního zařazení nebo instituce, ve které působí a identifikace oznamovaného;

d. jména a příjmení osob, včetně jejich kontaktních údajů, které mají informace o bezpečnostním incidentu;

e. informaci o tom, jak a případně od koho se o bezpečnostním incidentu oznamovatel dozvěděl;

f. informaci o tom, jak pravdivost zjištěných informací oznamovatel a zpracovatel ověřili;

g. zpracování osobních údajů, zpracovatelské operace a osobní údaje, kterých se bezpečnostní incident týká, včetně rozsah dotčených subjektů údajů;

h. možná rizika, která z bezpečnostního incidentu plynou vůči právům a svobodám subjektů údajů, správci, zpracovateli nebo třetím osobám.

K oznámení se připojí všechny důkazní prostředky, jimiž poskytovatel disponuje, které jej prokazují.

7. Oznámení se podává v českém jazyce.