Podmínky zpracování a zabezpečení osobních údajů – smlouva o zpracování

Článek I.
Úvodní prohlášení

1. Mezi stranami byla uzavřena smlouva o poskytování služeb. Tyto podmínky jsou součástí smlouvy podle věty první. Stanoví-li tyto podmínky něco jiného než smlouva, má smlouva přednost.
2. Těmito podmínkami smluvní strany plní povinnosti podle ust. čl. 28 obecného nařízení o ochraně osobních údajů.
3. Tyto podmínky upravují práva a povinnosti při zpracování osobních údajů, které je realizováno mezi smluvními stranami v pozici správce a zpracovatele osobních údajů tak, aby byla zajištěna maximální bezpečnost zpracovávaných osobních údajů a informací o jejich zabezpečení, stejně tak jako transparentnost zpracování, a aby byly řádně plněny jednotlivé povinnosti podle právní úpravy na ochranu osobních údajů.
4. Postavení smluvních stran v intencích správce – zpracovatel osobních údajů vyplývá ze smlouvy ve smyslu odst. 1, stejně jako úkoly zpracovatele v rámci zpracování.

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 rozumí:
   a. ***citlivým údajem*** – osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a dále genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby a údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby;
   b. ***veřejným subjektem*** – osoba zřízená zákonem, která plní zákonem stanovené úkoly ve veřejném zájmu;
   c. ***řetězením zpracovatelů –*** situace, kdy je do zpracování osobních údajů zapojena na základě dohody se zpracovatelem další osoba v pozici dílčího zpracovatele;
   d. ***dílčím zpracovatelem osobních údajů*** - zpracovatelem pověřená osoba k realizaci některého z úkonů zpracování osobních údajů, jež zpracovatel osobních údajů provádí pro správce osobních údajů, s níž má zpracovatel osobních údajů uzavřenu smlouvu o dílčím zpracování osobních údajů ve standardu odpovídajícím těmto podmínkám zejména z hlediska bezpečnosti zpracování osobních údajů, bezpečnosti informaci o jeho zabezpečení a plnění povinností podle obecného nařízení o ochraně osobních údajů a právní úpravy na ochranu osobních údajů obecně;
   e. ***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 a pro informace o parametrech zpracování;
   f. ***třetí zemí –*** každá země mimo členské státy Evropské unie;
   g. ***předáním osobních údajů do třetí země –*** předání osobních údajů do třetí země k realizaci jakékoli zpracovatelské operace, včetně využití služeb cloud computing, je-li služby byť jen částečně realizována ve třetí zemi;
   h. ***oznamovatel –*** člověk oznamující bezpečnostní incident;
   i. ***oznamovaný –*** člověk, který není oznamovatelem a dotýká se jej bezpečnostní incident ve smyslu, že je původcem nebo zavdal příčinu k bezpečnostnímu incidentu.

Článek III.
Základní parametry a podmínky zpracování osobních údajů
Práva a povinnosti stran

1. Zpracovatel bude dále pro správce osobních údajů zajišťovat a smluvní strany jsou v souvislosti se zpracováním osobních údajů oprávněn a povinni k následujícímu:

- **a.** poskytnout si veškerou nezbytnou součinnost k tomu, aby byly řádně plněny povinnosti plynoucí z právní úpravy na ochranu osobních údajů a aby bylo zajištěno odpovídající zabezpečení zpracovávaných osobních údajů a informací o jejich zabezpečení, stejně tak jako respektována práva a svobody subjektu údajů a v maximální možné míře usnadněno uplatňování práv ze strany subjektů údajů;
- **b.** zpracovatel osobních údajů bude zpracovávat osobní údaje pouze na základě doložených pokynů správce.
- **c.** pokud by mělo dojít v souvislosti se zpracováním osobních údajů ze strany zpracovatele osobních údajů k předání osobních údajů do třetích zemí, informuje o takovém záměru před jeho realizací zpracovatel osobních údajů správce v dostatečném časovém předstihu písemně nebo zprávou el. pošty s tím, aby se k záměru vyjádřil. Nevyjádří-li se správce do tří pracovních dnů ode dne doručení oznámení, platí, že s předáním osobních údajů do třetí země souhlasí. Nejde-li o členský stát EU, EHP, nebo o zemi označenou za bezpečnou zemi rozhodnutím Komise EU, ani o zemi, která ratifikovala Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních údajů nebo jiný případ, kdy by bylo předání mimo EU považováno podle rozhodnutí Komise EU za bezpečné, zajistí zpracovatel potřebnou úroveň ochrany (např. standardní smluvní doložky podle rozhodnutí Komise);
- **d.** zpracovatel osobních údajů přijme nezbytná technicko-organizační opatření k zajištění bezpečnosti zpracovávaných osobních údajů a informací o jejich zabezpečení, jakož i všechna další nezbytná opatření požadovaná čl. 32 obecného nařízení o ochraně osobních údajů v odpovídajícím standardu k zajištění bezpečnosti osobních údajů a informací o zabezpečení zpracování;
- **e.** zpracovatel osobních údajů zapojí do procesu zpracování osobních údajů dílčího zpracovatele pouze při splnění zde uvedených podmínek;
- **f.** zpracovatel osobních údajů poskytne správci osobních údajů nezbytnou součinnost při realizaci jeho povinností podle čl. 32 až 36 obecného nařízení;
- **g.** zpracovatel osobních údajů na pokyn správce osobních údajů zpracovávané osobní údaje nebo informace o zpracování osobních údajů zlikviduje, příp. opraví, upraví nebo aktualizuje;
- **h.** Uplatní-li subjekt údajů u zpracovatele osobních údajů jakékoli své právo, k němuž zpracovatel vůči subjektu údajů neplní za správce povinnosti správce osobních údajů, oznámí zpracovatel tuto skutečnost obratem správci osobních údajů a poskytne mu veškerou nezbytnou součinnost k tomu, aby správce osobních údajů mohl na uplatnění práva ze strany subjektu údajů řádně v právními předpisy stanovené lhůtě reagovat;
- **i.** zpracovatel bude vést záznamy o realizovaných zpracovatelských operacích a o souvisejících skutečnostech tak, aby správce osobních údajů byl schopen řádně prokázat plnění právními předpisy stanovených povinností tak, jak v rámci zásady odpovědnosti předvídá čl. 5 odst. 2 obecného nařízení o ochraně osobních údajů;
- **j.** zpracovatel bude při zpracování osobních údajů postupovat vždy tak, aby byly bezezbytku naplněny základní zásady a povinnosti v oblasti zpracování osobních údajů, jak plynou z čl. 5 odst. 1 obecného nařízení a z dalších článků jmenovaného právního předpisu, které odkazované ustanovení provádí a doplňují. Zpracovatel k tomuto účelu zavede zejména vhodné vnitřní procesy a opatření k zajištění odpovídající bezpečnosti zpracovávaných osobních údajů a informací o jejich zabezpečení, zajistí, aby se osoby oprávněné zpracovávat osobní údaje a osoby, které přichází do styku s informacemi o parametrech zpracování osobních údajů, či s informacemi o zabezpečení zpracování osobních údajů zavázaly k mlčenlivosti o těchto skutečnostech a informacích;
- **k.** při ukončení činnosti pro správce předá zpracovatel správci osobních údajů nebo určenému jinému zpracovateli osobních údajů zabezpečeným způsobem veškeré zpracovávané osobní údaje a veškeré související dokumenty a informace tak, aby bylo možné plynule a nerušně pokračovat v dalším zpracování osobních údajů, tj. zejména je-li zpracování osobních údajů prováděno prostřednictvím prostředků moderní techniky, budou údaje a související informace předány v otevřeném formátu tak, aby s nimi bylo možné dále pracovat a bylo je možné dále bez dalšího zpracovávat. Zpracovatel správci předá veškerou dokumentaci a informace nezbytné k řádnému prokázání legálnosti zpracování a plnění souvisejících povinností tak, aby byl správce později schopen prokázat legálnost zpracování a plnění souvisejících povinností zpětně po dobu odpovídající nejdelší promlčecí nebo prekluzivní lhůtě civilního nebo veřejnoprávního deliktu, který mohl být při zpracování realizovaném zpracovatelem spáchán a za něj by mohl správce (byť jen částečně) odpovídat;

l. shledá-li zpracovatel osobních údajů jakékoli nedostatky v podmínkách zpracování osobních údajů, které má zajišťovat správce osobních údajů, či ve zpracování osobních údajů jako takovém, či bude-li mít alespoň podezření na takové nedostatky, oznámí tuto skutečnost správci osobních údajů.

Článek IV.
Opatření k zabezpečení zpracovávaných osobních údajů

1. Míra bezpečnostních opatření k zabezpečení zpracovávaných osobních údajů a jejich nosičů či multimediálního prostředí, v němž jsou osobní údaje uloženy nebo zpracovávány, musí odpovídat povaze zpracovávaných osobních údajů a míře možného zásahu do práv subjektu údajů, jehož se týkají.

2. Bezpečnostní opatření jsou taková opatření, která slouží k zajištění důvěrnosti, čímž se míní zamezení zpřístupnění osobních údajů a jejich nosičů mimo okruh osob, jimž s ohledem na přidělená práva náleží realizovat s osobními údaji zpracovatelské operace, či s nimi jinak disponovat. Bezpečnostními opatřeními jsou dále i opatření sloužící vedle zamezení neoprávněného přístupu a zpracování osobních údajů i k zamezení neoprávněné změny, zničení, ztráty či výmazu (např. pořizování záloh).

3. Při určování okruhu oprávněných osoba a při přidělování kompetencí ve vztahu ke zpracovávaným osobním údajů se vychází z principu nezbytnosti a minimalizace, tj. oprávnění a jeho míra odvisí od osobou vykonávané pracovní pozice a kompetencí přidělených takové pracovní pozici, přičemž se oprávnění určí tak, aby měla dotyčná osoba možnost disponovat pouze s takovými osobními údaji, které jsou nezbytné k řádnému výkonu její funkce. Stejné platí i pro vymezení rozsahu zpracovatelských operací, ke kterým bude zmocněna a ohledně vymezení okruhu případů, kdy bude moci svá oprávnění vykonávat. Vždy je třeba dát konečného účelu zpracování osobních údajů.

4. Součástí řádného zabezpečení je i pravidelné prověřování efektivity a dostatečnosti přijatých bezpečnostních opatření, školení zaměstnanců a osob zapojených do zpracování osobních údajů a přicházejících do styku s informacemi o zpracování a o jeho zabezpečení a ověřování jejich znalostí, správného chápání fungování bezpečnostních pravidel a dodržování stanovených opatření a postupů.

5. Správci osobních údajů náleží právo buďto přímo nebo prostřednictvím třetí k tomu určené osoby provádět pravidelně audity a inspekce řádnosti plnění povinností zpracovatele osobních údajů, včetně oprávnění prověřovat dostatečnost přijatých opatření k zajištění bezpečnosti a dodržování opatření a postupů ze strany zaměstnanců zpracovatele.

6. Vytkne-li správce osobních údajů na základě kontroly/auditu/inspekce či na základě jiných zjištění zpracovateli nedostatky týkající se plnění jeho povinností, zjedná zpracovatel obratem nápravu. Zpracovatel o zjednání nápravy správce vyrozumí.

7. Uvedené v tomto článku platí pro zajištění bezpečnost informací o zabezpečení zpracování osobních údajů obdobně.

Článek V.
Další opatření k zabezpečení zpracovávaných osobních údajů

1. Bezpečnostní opatření zpracovatel provede na základě řádného zhodnocení rizik, jejich pravděpodobnosti a možných negativních důsledků z nich plynoucích pro práva a svobody subjektů údajů. 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 subjektů údajů.

2. Zpracovatel krom jiného zavede a bude garantovat mj. tato pravidla a principy určené k zajištění bezpečnosti zpracovaných osobních údajů a k jištění bezpečnosti jejich nosičů a multimediálních zařízení:

- **a.** povinnost počínat si tak, aby nedošlo ke ztrátě, zničení či neoprávněné změně anebo zpřístupnění zpracovávaných osobních údajů, anebo informací o jejich zabezpečení. V případě, že bezprostředně hrozí nebezpečí ztráty, neoprávněného zničení, změny či zpřístupnění osobních údajů nebo informací o jejich zabezpečení, povinnost v nezbytném rozsahu přiměřeným způsobem zakročit. O provedeném zákroku, jeho důvodech, průběhu a důsledcích bez zbytečného odkladu informovat;
- **b.** nikdo nesmí nakládat s osobními údaji a provádět zpracovatelské operace mimo rozsah svého zmocnění, mimo účel zpracování nebo bez toho, aby byl k předmětné zpracovatelské operaci naplněn právními předpisy uznaný důvod (právní titul) a byly řádně splněny i všechny ostatní právní povinnosti vyplývající z právních předpisů na ochranu osobních údajů;
- **c.** každý je povinen obratem zprávou elektronické pošty nebo písemně zpravit odpovědnou osobu o každé závadě v podmínkách či jednotlivých parametrech zpracování osobních údajů;
- **d.** zejména při zpracování osobních údajů prostřednictvím moderních technologií se zajistí pořizování záloh zpracovávaných osobních údajů a souvisejících informací a údajů o zpracování v takových časových

intervalech, aby byla zajištěna kontinuita zpracování a aktuálnost a přesnost zpracovávaných osobních údajů i v případě změny nebo zničení zpracovávaných osobních údajů; bude-li třeba zpracovávané osobní údaje obnovit ze zálohy, odpovědná osoba zajistí podle informací a záznamů o zpracování osobních údajů, aby bylo předmětné zpracování osobních údajů uvedeno do souladu s dříve realizovanými právy subjektů údajů, jakož i s dalšími zákonnými povinnostmi;

e. zajistí se i další vhodná a potřebná bezpečnostní opatření, například pravidelná vynucená změna přístupových hesel;

f. v maximální možné míře využívat technických a jiných možností zabezpečení, kterými jsou opatřeny pracovní a jiné prostředky, kterých se využívá ke zpracování osobních údajů, 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;

Uvedené v tomto odstavci platí pro zajištění bezpečnost informací o zabezpečení zpracování osobních údajů obdobně

Článek VI.
Komunikace

1. Komunikace (telefonem, elektronickou poštou, běžnou poštou) související se zpracováním osobních údajů, 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 osobních údajů, neměl možnost seznámit nikdo jiný než její oprávněný adresát.

2. K předávání osobních údajů 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 výlučně systém datových schránek. V těchto případech není možné sdělit osobní údaje telefonicky, elektronickou poštou nebo jinak.

4. Není-li možné k předání údajů využít systému datových schránek, lze využít 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 osobních údajů prostřednictvím zprávy el. pošty je možné jedině při řádném zabezpečení předávaných osobních údajů. 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. Odpovědní zástupci stran si zvolí bezpečné heslo a toto si diskrétně sdělí.
7. K předávání osobních údajů lze užít telefonního spojení pouze výjimečně; telefonním spojením se míní i SMS, MMS či mobilní aplikace plnící obdobnou funkci. Prostřednictvím telefonního spojení lze poskytovat osobní údaje pouze tehdy, je-li bezpečně ověřena totožnost volajícího, je-li jisté, že hovoru nemůže být účastna jiná osoba než řádně identifikovaný volající, a v případě, kdy dochází k předávání údajů mezi správcem a zpracovatelem, příp. mezi správcem a správcem, nebo zpracovatelem a dílčím zpracovatelem, je-li jisté, že údaje jsou řádně zanášeny do příslušné evidence. Je-li k předání údajů užita SMS, MMS nebo aplikace plnící obdobnou funkci, musí být zpráva po zanesení údajů do evidence neprodleně smazána.

Článek VII.
Bezpečnostní incident

1. Dozví-li se zpracovatel osobních údajů o bezpečnostním incidentu, je povinen jej bezodkladně oznámit správci osobních údajů. 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) na straně správce, oznamované osoby, či jiných dotčených osob (rodinných příslušníků oznamovaného atp.).
3. Bezpečnostní incident se diskrétně oznamuje správcem určené osobě.
4. Zpracovatel osobních údajů zajistí, aby oznamovatel vždy oznamoval tak, dotýká-li se oznámení některého se spoluzaměstnanců nebo členů zpracovatele 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 zpracovatel disponuje, které jej prokazují; čl. VII. platí i zde.
7. Oznámení se podává v českém jazyce.

Článek VIII.
Podmínky zapojení dílčího zpracovatele

1. Zpracovatel osobních údajů je oprávněn do procesu zpracování osobních údajů zapojit dílčího zpracovatele osobních údajů.
2. Dílčím zpracovatelem osobních údajů může být taková osoba, která bude poskytovat dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky podle právní úpravy na ochranu osobních údajů a byla zajištěna bezpečnost a ochrana osobních údajů, práv a svobod subjektů údajů. Zpracovatel osobních údajů odpovídá za řádné prověření spolehlivosti dílčího zpracovatele osobních údajů, kterého má zájem zapojit do zpracování osobních údajů.
3. Záměr zapojit do zpracování osobních údajů dílčího zpracovatele osobních údajů oznámí zpracovatel osobních údajů písemně správci osobních údajů. Správci osobních údajů svědčí právo na námitku vůči zapojení dílčího zpracovatele osobních údajů, resp. správci osobních údajů se vyhrazuje právo schválit osobu dílčího zpracovatele.

Nevyrozumí-li správce osobních údajů o svém rozhodnutí stran připuštění zapojení dílčího zpracovatele do zpracování osobních údajů do 5 pracovní dní ode dne doručení vyrozumění o zájmu na zapojení dílčího zpracovatele osobních údajů, platí, že zpracovatel osobních údajů daného dílčího zpracovatele osobních údajů do procesu zpracování osobních údajů zapojit může.

4. Zpracovatel osobních údajů zaváže dílčího zpracovatele k plnění povinností podle právní úpravy na ochranu osobních údajů a k zajištění bezpečnosti zpracovávaných osobních údajů a informací o jejich zabezpečení nejméně v rozsahu dle těchto podmínek. Stejné platí i o dalším obsahu těchto podmínek.
5. Zpracovatel osobních údajů odpovídá správci osobních údajů za činnost dílčího zpracovatele osobních údajů tak, jako by zpracovatel osobních údajů pro správce osobních údajů plnil předmětnou povinnost, resp. realizoval danou činnost sám.

Článek IX.
Společná ujednání

1. Zpracovatel k výzvě správce osobních údajů zpřístupní bez zbytečného odkladu správci osobních údajů nebo jím určené osobě zpracovávané osobní údaje nebo jejich určenou část, stejně tak jako informace o zpracování osobních údajů, včetně informací o jejich zabezpečení.
2. Zpracovatel k výzvě správce osobních údajů předá bez zbytečného odkladu správci nebo jím určené jiné osobě kopii zpracovávaných osobních údajů způsobem a ve formátu, aby bylo předané osobní údaje dále zpracovávat. Stejné platí pro informace o zpracování osobních údajů a o jejich zabezpečení.
3. Zpracovatel k výzvě správce osobních údajů předloží správci bez zbytečného odkladu dokumentaci prokazující, že se zpracování osobních údajů realizované zpracovatelem ve prospěch správce zakládá na odpovídajícím a platném právním titulu.

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.