Podmienky spracovania a zabezpečenie osobných údajov – zmluva o spracovanie

Článok I.
Úvodné prehlásenie

1. Medzi stranami bola uzavretá zmluva o poskytovaní služieb. Tieto podmienky sú súčasťou zmluvy podľa vety prvej. Ak stanovuje tieto podmienky niečo iné než zmluva, má zmluva prednosť.
2. Týmito podmienkami zmluvné strany plnia povinnosti podľa ust. čl. 28 všeobecného nariadenia o ochrane osobných údajov.
3. Tieto podmienky upravujú práva a povinnosti pri spracovaní osobných údajov, ktoré je realizované medzi zmluvnými stranami v pozícii správcu a spracovateľa osobných údajov tak, aby bola zaistená maximálna bezpečnosť spracovávaných osobných údajov a informácií o ich zabezpečení, rovnako tak ako transparentnosť spracovania, a aby boli riadne plnené jednotlivé povinnosti podľa právnej úpravy na ochranu osobných údajov.
4. Postavenie zmluvných strán v intenciách správcu – spracovateľ osobných údajov vyplýva zo zmluvy v zmysle odst. 1, rovnako ako úlohy spracovateľa v rámci spracovania.

Článok II.
Vymedzenie pojmov

1. Ak nie je vyslovene stanovené inak, majú pojmy vymedzené v čl. 4 všeobecného nariadenia o ochrane osobných údajov zhodný význam, ktorý im je prisúdený odkazovaným ustanovením všeobecného nariadenia.
2. Ďalej sa rozumie:
   a. ***citlivým údajom*** – osobné údaje, ktoré vypovedajú o rasovom či etnickom pôvode, politických názoroch, náboženskom vyznaní či filozofickom presvedčení alebo členstvo v odboroch, a ďalšie genetické údaje, biometrické údaje za účelom jedinečnej identifikácie fyzickej osoby a údaje o zdravotnom stave či o sexuálnom živote alebo sexuálnej orientácii fyzickej osoby;
   b. ***verejným subjektom*** – osoba zriadená zákonom, ktorá plní zákonom stanovené úlohy vo verejnom záujme;
   c. ***reťazením spracovateľov –*** situácie, keď je do spracovania osobných údajov zapojená na základe dohody so spracovateľom ďalšia osoba v pozícii dielčieho spracovateľa;
   d. ***dielčím spracovateľom osobných údajov*** - spracovateľom poverená osoba k realizácii niektorého z úkonov spracovania osobných údajov, ktoré spracovateľ osobných údajov vykonáva pre správcu osobných údajov, s ktorou má spracovateľ osobných údajov uzavretú zmluvu o dielčom spracovaní osobných údajov v štandarde zodpovedajúcim týmto podmienkam hlavne z hľadiska bezpečnosti spracovania osobných údajov, bezpečnosti informácii o jeho zabezpečení a plnení povinností podľa všeobecného nariadenia o ochrane osobných údajov a právnej úpravy na ochranu osobných údajov všeobecne;
   e. ***bezpečnostným incidentom -*** porušenie zabezpečenia osobných údajov, ktoré vedie k náhodnému alebo protiprávnemu zničeniu, strate, zmene alebo neoprávnenému poskytnutiu alebo sprístupnenie prenášaných, uložených alebo inak spracovávaných osobných údajov, alebo aspoň ohrozenia náhodným alebo protiprávnym zničením, stratou, zmenou alebo neoprávneným poskytnutím alebo sprístupneným osobných údajov, ďalej napríklad aj strata alebo neoprávnené sprístupnenie hesla, príp. prístupových údajov či prostriedkov do priestoru spracovania osobných údajov, k uloženým či spracovávaným osobným údajom, do multimediálnych prostriedkov a prostriedkov výpočtovej techniky určených ku spracovaniu osobných údajov alebo k ich uloženiu; uvedené platí obdobne aj pre informácie o zabezpečení spracovania osobných údajov a pre informácie o parametroch spracovania;
   f. ***Tretie krajiny –*** každá krajina mimo členské štáty Európskej únie;
   g. ***poskytnutím osobných údajov do tretích krajín -*** poskytnutím osobných údajov do tretích krajín k realizácii akéhokoľvek spracovateľskej operácie, vrátane využitia služieb cloud computing, ak je služba čo i len čiastočne realizovaná v tretích krajinách;
   h. ***oznamovateľ –*** človek oznamujúci bezpečnostný incident;
   i. ***oznamovaný –*** človek, ktorý nie je oznamovateľom a dotýka sa jej bezpečnostný incident v zmysle, že je pôvodcom alebo dal príčinu k bezpečnostnému incidentu.

Článok III.
Základné parametre a podmienky spracovania osobných údajov
Práva a povinnosti strán

1. Spracovateľ bude ďalej pre správcu osobných údajov zaisťovať a zmluvné strany sú v súvislosti so spracovaním osobných údajov oprávnený a povinný k nasledujúcemu:

a. poskytnúť si každú nevyhnutnú súčinnosť k tomu, aby boli riadne plnené povinnosti plynúce z právnej úpravy na ochranu osobných údajov a aby bolo zaistené zodpovedajúce zabezpečenie spracovávaných osobných údajov a informácií o ich zabezpečení, rovnako tak ako rešpektované práva a slobody subjektu údajov a v maximálnej možnej miere uľahčené uplatňovanie práv zo strany subjektov údajov;

b. spracovateľ osobných údajov bude spracovávať osobné údaje len na základe doložených pokynov správcu.

c. pokiaľ by malo dôjsť v súvislosti so spracovaním osobných údajov zo strany spracovateľa osobných údajov k poskytnutiu osobných údajov do tretích krajín, informuje o takom zámere pred jeho realizáciou spracovateľ osobných údajov správcu v dostatočnom časovom predstihu písomne alebo správou el. pošty s tým, aby sa k zámeru vyjadril. Nevyjadrí sa správca do troch pracovných dní odo dňa doručenia oznámenia, platí, že s poskytnutím osobných údajov do tretích krajín súhlasí. Ak sa nejedná o členský štát EÚ, EHP, alebo o krajinu označenú za bezpečnú krajinu rozhodnutím Komisie EÚ, ani o krajinu, ktorá ratifikovala Dohovor o ochrane osôb so zreteľom na automatizované spracovanie osobných údajov alebo iný prípad, keď by bolo poskytnutie mimo EÚ považované podľa rozhodnutia Komisie EÚ za bezpečné, zaistí spracovateľ potrebnú úroveň ochrany (napr. štandardnej zmluvnej doložky podľa rozhodnutia Komisie);

d. spracovateľ osobných údajov prijme nevyhnutné technicko-organizačné opatrenia k zaisteniu bezpečnosti spracovávaných osobných údajov a informácií o ich zabezpečení, tak ako aj všetky ďalšie nevyhnutné opatrenia požadované čl. 32 všeobecného nariadenia o ochrane osobných údajov v zodpovedajúcom štandarde k zaisteniu bezpečnosti osobných údajov a informácii o zabezpečení spracovania;

e. spracovateľ osobných údajov zapojí do procesu spracovania osobných údajov dielčieho spracovateľa len pri splnení tu uvedených podmienok;

f. spracovateľ osobných údajov poskytne správcovi osobných údajov nevyhnutnú súčinnosť pri realizácii jeho povinností podľa čl. 32 až 36 všeobecného nariadenia;

g. spracovateľ osobných údajov na pokyn správcu osobných údajov spracovávané osobné údaje alebo informácie o spracovaní osobných údajoch zlikviduje, príp. opraví, upraví alebo aktualizuje;

h. Ak si uplatní subjekt údajov u spracovateľa osobných údajov akékoľvek svoje právo, ku ktorému spracovateľ voči subjektu údajov neplní za správcu povinnosti správcu osobných údajov, oznámi spracovateľ túto skutočnosť obratom správcovi osobných údajov a poskytne mu všetku nevyhnutnú súčinnosť k tomu, aby správca osobných údajov mohol na uplatnenie práva zo strany subjektu údajov riadne v právnymi predpismi stanovenej lehote reagovať;

i. spracovateľ bude viesť záznamy o realizovaných spracovateľských operáciách a o súvisiacich skutočnostiach tak, aby správca osobných údajov bol schopný riadne preukázať plnenie právnych predpisov stanovených povinností tak, ako v rámci zásady zodpovednosti predvída čl. 5 odst. 2 všeobecného nariadenia o ochrane osobných údajov;

j. spracovateľ bude pri spracovaní osobných údajov postupovať vždy tak, aby boli bezodkladne naplnené základné zásady a povinnosti v oblasti spracovania osobných údajov tak, ako plynú z čl. 5 odst. 1 všeobecného nariadenia a z ďalších článkov menovaného právneho predpisu, ktoré odkazované ustanovenia vykonáva a doplňuje. Spracovateľ k tomuto účelu zavedie najmä vhodné vnútorné procesy a opatrenia k zaisteniu zodpovedajúcej bezpečnosti spracovávaných osobných údajov a informácii o ich zabezpečení, zaistí, aby sa osoby oprávnené spracovávať osobné údaje a osoby, ktoré prichádzajú do styku s informáciami o parametroch spracovania osobných údajov, či s informáciami o zabezpečení spracovania osobných údajov zaviazali k mlčanlivosti o týchto skutočnostiach a informáciách;

k. pri ukončení činnosti pre správcu poskytne spracovateľ správcovi osobných údajov alebo určenému inému spracovateľovi osobných údajov zabezpečeným spôsobom všetkých spracovávaných osobných údajov a všetky súvisiace dokumenty a informácie tak, aby bolo možné plynule a nerušene pokračovať v ďalšom spracovaní osobných údajov, tj. najmä ak je spracovanie osobných údajov vykonávané prostredníctvom prostriedkov modernej techniky, budú údaje a súvisiace informácie odovzdané v otvorenom formáte tak, aby s nimi bolo možné ďalej pracovať a bolo ich možné ďalej bez ďalšieho spracovávať. Spracovateľ správcovi odovzdá všetku dokumentáciu a informácie nevyhnutné k riadnemu preukázanie legálnosti spracovania a plnenia súvisiacich povinností tak, aby bol správca neskôr schopný preukázať legálnosť spracovania a plnenia

súvisiacich povinností spätne po dobu zodpovedajúcej najdlhšej premlčacej alebo prekluzívnej lehote civilného alebo verejnoprávneho deliktu, ktorý mohol byť pri spracovaní realizovanom spracovateľom spáchaný a za neho by mohol správca (hoci len čiastočne) zodpovedať;

l. ak zistí spracovateľ osobných údajov akékoľvek nedostatky v podmienkach spracovania osobných údajov, ktoré má zaisťovať správca osobných údajov, či v spracovaní osobných údajov ako takom, ak bude mať aspoň podozrenie na také nedostatky, oznámi túto skutočnosť správcovi osobných údajov.

Článok IV.
Opatrenie k zabezpečeniu spracovávaných osobných údajov

1. Miera bezpečnostných opatrení k zabezpečeniu spracovávaných osobných údajov a ich nosičov či multimediálneho prostredia, v ktorom sú osobné údaje uložené alebo spracovávané, musí zodpovedať povahe spracovávaných osobných údajov a miere možného zásahu do práv subjektu údajov, ktorého sa týkajú.

2. Bezpečnostné opatrenia sú také opatrenia, ktoré slúžia k zaisteniu dôvernosti, čím sa rozumie zamedzeniu sprístupneniu osobných údajov a ich nosičov mimo okruh osôb, ktorým s ohľadom na pridelené práva náleží realizovať s osobnými údajmi spracovateľskej operácie, či s nimi inak disponovať. Bezpečnostnými opatreniami sú ďalej aj opatrenia slúžiace vedľa zamedzenia neoprávneného prístupu a spracovania osobných údajov aj k zamedzeniu neoprávnenej zmeny, zničeniu, straty či výmazu (napr. robenie záloh).

3. Pri určovaní okruhu oprávnených osôb a pri prideľovaní kompetencií vo vzťahu ku spracovávaným osobným údajom sa vychádza z princípu nevyhnutnosti a minimalizácie, tj. oprávnenie a jeho miera závisí od osobou vykonávanej pracovnej pozície a kompetencií pridelených takej pracovnej pozícii, pričom sa oprávnenie určí tak, aby mala dotyčná osoba možnosť disponovať len s takými osobnými údajmi, ktoré sú nevyhnutné k riadnemu výkonu jej funkcie. Rovnako platí aj pre vymedzenie rozsahu spracovateľských operácii, ku ktorým bude zmocnená a ohľadne vymedzenia okruhu prípadov, kedy bude môcť svoje oprávnenie vykonávať. Vždy je treba dať konečný účel spracovania osobných údajov.

4. Súčasťou riadneho zabezpečenia je aj pravidelné preverovanie efektivity a dostatočnosti prijatých bezpečnostných opatrení, školenie zamestnancov a osôb zapojených do spracovania osobných údajov a prichádzajúcich do styku s informáciami o spracovaní a o jeho zabezpečení a overovaní ich znalostí, správneho chápania fungovaní bezpečnostných pravidiel a dodržiavanie stanovených opatrení a postupov.

5. Správcovi osobných údajov náleží právo buďto priamo alebo prostredníctvom tretej k tomu určenej osoby vykonávať pravidelné audity a inšpekcie riadnosti plnenia povinností spracovateľa osobných údajov, vrátane oprávnenia preverovať dostatočnosť prijatých opatrení k zaisteniu bezpečnosti a dodržiavanie opatrení a postupov zo strany zamestnancov spracovateľa.

6. Ak vytkne správca osobných údajov na základe kontroly/auditu/inšpekcie či na základe iných zistení spracovateľovi nedostatky týkajúce sa plnenia jeho povinností, zjedná spracovateľ obratom nápravu. Spracovateľ o zjednaní nápravy správcu vyrozumie.

7. Uvedené v tomto článku platí pre zaistenie bezpečnosti informácií o zabezpečení spracovania osobných údajov obdobne.

Článok V.
Ďalšie opatrenia k zabezpečeniu spracovávaných osobných údajov

1. Bezpečnostné opatrenia spracovateľ vykoná na základe riadneho zhodnotenia rizík, ich pravdepodobnosti a možných negatívnych dôsledkov z nich plynúcich pre práva a slobody subjektov údajov. Primárnym cieľom musí byť eliminovať riziká, tam kde to nie je možné následne riziká minimalizovať, a kde nie je ani to možné, eliminovať alebo aspoň minimalizovať možné negatívne dôsledky pre práva a slobody subjektov údajov.

2. Spracovateľ okrem iného zavedie a bude garantovať oi. tieto pravidla a princípy určené k zaisteniu bezpečnosti spracovaných osobných údajov a k zaisteniu bezpečnosti ich nosičov a multimediálnych zariadení:

- **a.** povinnosť počínať si tak, aby nedošlo k strate, zničeniu či neoprávnenej zmene alebo sprístupneniu spracovávaných osobných údajov, alebo informácií o ich zabezpečení. V prípade, že bezprostredne hrozí nebezpečenstvo straty, neoprávneného zničenia, zmeny či sprístupneniu osobných údajov alebo informácií o ich zabezpečení, povinnosť v nevyhnutnom rozsahu primeraným spôsobom zakročiť. O uskutočnenom zákroku, jeho dôvodoch, priebehu a dôsledkoch bez zbytočného odkladu informovať;
- **b.** nikto nesmie nakladať s osobnými údajmi a vykonávať spracovateľské operácie mimo rozsah svojho mocenstva, mimo účel spracovania alebo bez toho, aby bol k predmetnej spracovateľskej operácii naplnený právnymi predpismi uznaný dôvod (právny titul) a boli riadne splnené aj všetky ostatné právne povinnosti vyplývajúce z právnych predpisov na ochranu osobných údajov;

c. každý je povinný obratom správou elektronickej pošty alebo písomne spraviť zodpovednú osobu o každej závade v podmienkach či jednotlivých parametroch spracovania osobných údajov;

d. najmä pri spracovaní osobných údajov prostredníctvom moderných technológií sa zaistí obstarávanie záloh spracovávaných osobných údajov a súvisiacich informácii a údajov o spracovaní v takých časových intervaloch, aby bola zaistená kontinuita spracovania a aktuálnosť a presnosť spracovávaných osobných údajov aj v prípade zmeny alebo zničenia spracovávaných osobných údajov; ak bude nutné spracovávané osobné údaje obnoviť zo zálohy, zodpovedná osoba zaistí podľa informácii a záznamu o spracovaní osobných údajov, aby bolo predmetné spracovanie osobných údajov uvedené do súladu so skôr realizovanými právami subjektov údajov, ako aj s ďalšími zákonnými povinnosťami;

e. zaistia sa aj ďalšie vhodné a potrebné bezpečnostné opatrenia, napríklad pravidelná vynútená zmena prístupových hesiel;

f. v maximálnej možnej miere využívať technických a iných možností zabezpečenia, ktorými sú zabezpečené pracovné a iné prostriedky, ktoré sa využívajú ku spracovaniu osobných údajov, najmä sa zaistí povinnosť zamestnancov:

- **i.** uzamykanie miestností, skríň a iných priestorov, v ktorých sú uložené nosiče osobných údajov, ak nie je v priestoroch prítomný nikto oprávnený pristúpiť k predmetným osobným údajom a ich nosičom;
- **ii.** pri skončení práce s technickým či multimediálnym zariadením alebo aplikáciami odhlásenia z tohoto zaradenia, prostredia či aplikácie;
- **iii.** dôsledné utajovanie hesiel a prihlasovacích kódov pre prístup do zariadení, multimediálneho prostredia či do jednotlivých aplikácií;
- **iv.** voliť bezpečné heslá, tj. heslá pozostávajúce z najmenej 8 alfanumerických i nealfanumerických znakov, kde každé heslo musí obsahovať veľké a malé písmená;
- **v.** v prípade mobilných telefónov a iných obdobných zariadení vždy zvoliť zabezpečenie pre spustenie a prihlásenie do zariadenia, rovnako ako pre jeho odomknutie, aspoň prostredníctvom zadaním štvormiestneho PIN; ak je to možné, zvolí sa vždy aj vyšší spôsob zabezpečenia;
- **vi.** na multimediálnom zariadení a výpočtovej techniky, ktorá bola zamestnancovi zverená k plneniu pracovných úloh, bez povolenia a asistencie zodpovednej osoby neinštalovať akýkoľvek software, či nevykonávať akékoľvek zmeny, najmä potom vyraďovať antivírové a či iné obdobné programy určené k zaisteniu bezpečnosti spracovávaných osobných údajov;
- **vii.** ak je zamestnancovi zverený mobilný telefón alebo služobný PC, či iné obdobné multimediálne zariadenia či zariadenia výpočtovej techniky, najmä, ak má zamestnanec možnosť disponovať s ním i mimo priestory zamestnávateľa, aby dotyčný prijal a dôsledne vykonal také opatrenia, aby úplne vylúčil prístup a dispozíciu s týmito prostriedkami zo strany akejkoľvek tretej osoby, rovnako tak ako opatrenia k tomu, aby predišiel zničeniu alebo poškodeniu takých zariadení;

Uvedené v tomto odstavci platí pre zaistenie bezpečnosti informácii o zabezpečení spracovania osobných údajov obdobne.

Článok VI.
Komunikácia

1. Komunikácia (telefónom, elektronickou poštou, bežnou poštou) súvisiaca so spracovaním osobných údajov, ak je vykonaná v rámci jednej zo strán alebo medzi nimi či voči tretím osobám (zmluvným partnerom, klientom, štátnym úradom atď.), sa realizuje vždy maximálne bezpečne a diskrétne, tj. tak, aby sa s obsahom správy, vrátane poskytovania osobných údajov, nemal možnosť zoznámiť nikto iný než jej oprávnený adresát.

2. K poskytovaniu osobných údajov slúži: dátová schránka, správa el. pošty, úložné el. služby, alebo doručovanie prostredníctvom poskytovateľa poštovných služieb, príp. iný obdobný spôsob doručovania, kde dochádza k fyzickému poskytnutiu nosiča osobných údajov adresátovi (služby messengera atp.).

3. Ak je to s ohľadom na povahu adresáta a poskytovanej služby možné, použije sa na komunikáciu výlučne systém dátových schránok. V týchto prípadoch nie je možné zdieľať osobné údaje telefonicky, elektronickou poštou alebo inak.

4. Ak nie je možné k poskytnutiu údajov využiť systému dátových schránok, je možné využiť el. poštu alebo poskytovateľa poštovných služieb, príp. inú obdobnú službu, kde dochádza k fyzickému poskytnutiu nosiča údajov (služba messengera atp.). V týchto prípadoch je potrebné vždy určiť konkrétneho adresáta a využiť služby potvrdenia doručenia, resp. doručenia do vlastných rúk.

5. Poskytnutie osobných údajov prostredníctvom správy el. pošty je možné jedine pri riadnom zabezpečení poskytovaných osobných údajov. Zabezpečením sa rozumie najmenej komprimácia poskytovaného súboru do formátu *.zip alebo podobného formátu a kódovanie predmetného súboru prostredníctvom bezpečného hesla.

Bezpečným heslom sa rozumie heslo najmenej o 8 znakoch, ktoré obsahuje alfanumerické (veľké a malé písmená a číslice) i nealfanumerické znaky. Heslo musí byť s adresátom dohodnuté vopred. Heslo musí byť bezpečne poskytnuté – bezpečným poskytnutím nie je poskytnutie hesla v otvorenej správe el. pošty; rovnako to platí pre zmenu hesla.

6. Zodpovední zástupcovia strán si zvolia bezpečné heslo a toto si diskrétne zazdieľajú.
7. K poskytovaniu osobných údajov je možné použiť telefonické spojenie len výnimočne; telefonickým spojením sa rozumie aj SMS, MMS či mobilní aplikácie plniace obdobnú funkciu. Prostredníctvom telefonického spojenia je možné poskytovať osobné údaje len vtedy, ak je bezpečne overená totožnosť volajúceho, ak je isté, že na hovore nemôže byť zúčastnená iná osoba než riadne identifikovaný volajúci, a v prípade, kedy dochádza k poskytovaniu údajov medzi správcom a spracovateľom, príp. medzi správcom a správcom, alebo spracovateľom a dielčím spracovateľom, ak je isté, že údaje sú riadne zanesené do príslušnej evidencie. Ak je k poskytnutiu údajov použitá SMS, MMS alebo aplikácia plniaca obdobnú funkciu, musí byť správa po zanesení údajov do evidencie bezodkladne zmazaná.

Článok VII.
Bezpečnostný incident

1. Ak sa dozvie spracovateľ osobných údajov o bezpečnostnom incidente, je povinný ho bezodkladne oznámiť správcovi osobných údajov. Rovnako platí aj o dôvodnom podozrení na bezpečnostný incident.
2. Predpokladom oznámenia v zmysle tohto článku je vždy:
   a) poctivosť na strane oznamovateľa;
   b) presvedčenie oznamovateľa o pravdivosti oznámenia;
   c) presvedčenie oznamovateľa o legálnosti jednania/oznámenia;
   d) overenie oznamovaných informácií.

   Iné oznámenie (neoverené, nepoctivé – vedené s úmyslom niekoho poškodiť) môžu zakladať povinnosti nahradiť ujmu (hmotnú alebo nehmotnú) na strane správcu, oznamovanej osoby, či iných dotknutých osôb (rodinných príslušníkov oznamovaného atp.).
3. Bezpečnostný incident sa diskrétne oznamuje správcom určenej osobe.
4. Spracovateľ osobných údajov zaistí, aby oznamovateľ vždy oznamoval tak, ak sa dotýka oznámenie niektorého zo spoluzamestnancov alebo členov spracovateľa alebo inej osoby, kde taká osoba má mať postavenie porušiteľa právnych povinností, aby sa o oznámení nedozvedel oznamovaný.
5. Oznámenie sa podáva písomne alebo prostredníctvom správy el. pošty.
6. V oznámení sa uvedie (ak to bude z povahy veci možné):
   a. meno a priezvisko, pracovné zaradenie a kontaktné údaje oznamovateľa;
   b. všetko, čo o oznamovanom bezpečnostnom incidente oznamovateľ a tretie osoby vedia (popis bezpečnostného incidentu);
   c. mená a priezviská všetkých osôb, ktoré sa bezpečnostného incidentu zúčastnili, vrátane ich pracovného zaradenia alebo inštitúcie, v ktorej pôsobí a identifikácie oznamovaného;
   d. mená a priezviská osôb, vrátane ich kontaktných údajov, ktoré majú informácie o bezpečnostnom incidente;
   e. informácie o tom, ako a prípadne od koho sa o bezpečnostnom incidente oznamovateľ dozvedel;
   f. informácie o tom, ako pravdivosť zistených informácií oznamovateľ a spracovateľ overili;
   g. spracovanie osobných údajov, spracovateľské operácie a osobné údaje, ktorých sa bezpečnostný incident týka, vrátane rozsahu dotknutých subjektov údajov;
   h. možné riziká, ktoré z bezpečnostného incidentu plynú voči právam a slobodám subjektov údajov, správcov, spracovateľom alebo tretím osobám.

   K oznámeniu sa pripoja všetky dôkazné prostriedky, ktorými spracovateľ disponuje, ktoré ho preukazujú; čl. VII. platí aj tu.
7. Oznámenie sa podáva v(českom) slovenskom jazyku.

Článok VIII.
Podmienky zapojenia dielčieho spracovateľa

1. Spracovateľ osobných údajov je oprávnený do procesu spracovania osobných údajov zapojiť dielčieho spracovateľa osobných údajov.
2. Dielčím spracovateľom osobných údajov môže byť taká osoba, ktorá bude poskytovať dostatočné záruky zavedenia vhodných technických a organizačných opatrení tak, aby dané spracovanie spĺňalo požiadavky podľa právnej úpravy na ochranu osobných údajov a bola zaistená bezpečnosť a ochrana osobných údajov, práv a slobôd

subjektov údajov. Spracovateľ osobných údajov zodpovedá za riadne preverenie spoľahlivosti dielčieho spracovateľa osobných údajov, ktorého má záujem zapojiť do spracovania osobných údajov.

3. Zámer zapojiť do spracovania osobných údajov dielčieho spracovateľa osobných údajov oznámi spracovateľ osobných údajov písomne správcovi osobných údajov. Správcovi osobných údajov prislúcha právo na námietku voči zapojeniu dielčieho spracovateľa osobných údajov, resp. správcovi osobných údajov sa vyhradzuje právo schváliť osobu dielčieho spracovateľa. Ak nevyrozumie správca osobných údajov o svojom rozhodnutí strany pripustením zapojenia dielčieho spracovateľa do spracovania osobných údajov do 5 pracovných dní odo dňa doručenia vyrozumenia o záujme na zapojenie dielčieho spracovateľa osobných údajov, platí, že spracovateľ osobných údajov daného dielčieho spracovateľa osobných údajov do procesu spracovania osobných údajov zapojiť môže.
4. Spracovateľ osobných údajov zaviaže dielčieho spracovateľa k plneniu povinností podľa právnej úpravy na ochranu osobných údajov a k zaisteniu bezpečnosti spracovávaných osobných údajov a informácii o ich zabezpečení najmenej v rozsahu podľa týchto podmienok. Rovnako platí aj o ďalšom obsahu týchto podmienok.
5. Spracovateľ osobných údajov zodpovedá správcovi osobných údajov za činnosť dielčieho spracovateľa osobných údajov tak, ako by spracovateľ osobných údajov pre správcu osobných údajov plnil predmetnú povinnosť, resp. realizoval danú činnosť sám.

Článok IX.
Spoločné ustanovenia

1. Spracovateľ k výzve správcovi osobných údajov sprístupní bez zbytočného odkladu správcovi osobných údajov alebo im určenej osobe spracovávané osobné údaje alebo ich určenú časť, rovnako tak ako informácie o spracovaní osobných údajov, vrátane informácii o ich zabezpečení.
2. Spracovateľ k výzve správcu osobných údajov poskytne bez zbytočného odkladu správcovi alebo im určenej inej osobe kópiu spracovávaných osobných údajov spôsobom a vo formáte, aby boli odovzdané osobné údaje ďalej spracovávať. Rovnako platí pre informácie o spracovaní osobných údajov a o ich zabezpečení.
3. Spracovateľ k výzve správcu osobných údajov predloží správcovi bez zbytočného odkladu dokumentáciu preukazujúcu, že so spracovaním osobných údajov realizovaným spracovateľom v prospech správcu zakladá na zodpovedajúcom a platnom právnom titule.

Podmienky zabezpečenia, diskrétnosti a oznamovanie bezpečnostných incidentov

Článok I.
Prehlásenie

1. Poskytovateľ sa zaviazal príjemcovi poskytnúť dohodnutú službu či dodať dohodnutý tovar.
2. Predmetom poskytovanej služby nie je žiadna spracovateľská operácia zo strany poskytovateľa vo vzťahu k príjemcovi spracovávaným osobným údajom. Hoci nie je vylúčené, že poskytovateľ príde pri svojej činnosti pre príjemcu do kontaktu s osobnými údajmi, informáciami o parametroch spracovania osobných údajov, vrátane informácií o zabezpečenie, nie je oprávnený s nimi akokoľvek disponovať.
3. Tieto podmienky sú súčasťou zmluvy podľa odst. 1. ak stanovuje zmluva niečo iné než tieto podmienky, má zmluva prednosť.

Článok II.
Vymedzenie pojmov

1. Ak nie je výslovne stanovené inak, majú pojmy vymedzené v čl. 4 všeobecného nariadenia o ochrane osobných údajov zhodný význam, ktorý im je prisúdený odkazovaným ustanovením všeobecného nariadenia.
2. Ďalej sa pre účely tejto zmluvy rozumie:
   a. ***bezpečnostným incidentom*** **-** porušenie zabezpečenia osobných údajov, ktoré vedie k náhodnému alebo protiprávnemu zničeniu, strate, zmene alebo neoprávnenému poskytnutiu alebo sprístupneniu prenášaných, uložených alebo inak spracovávaných osobných údajov, alebo aspoň ohrozenie náhodným alebo protiprávnym zničením, stratou, zmenou alebo neoprávneným poskytnutím alebo sprístupneným osobných údajov, ďalej napríklad aj strata alebo neoprávnené sprístupnenie hesla, príp. prístupových údajov či prostriedkov do priestorov spracovania osobných údajov, k uloženým či spracovávaným osobným údajom, do multimediálnych prostriedkov a prostriedkov výpočtovej techniky určenej k spracovaniu osobných údajov alebo k ich uloženiu; uvedené platí obdobne aj pre informácie o zabezpečení spracovanie osobných údajov;
   b. ***oznamovateľ*** **–** človek oznamujúci bezpečnostný incident;
   c. ***oznamovaný*** **–** človek, ktorý nie je oznamovateľom a dotýka sa ho bezpečnostný incident v zmysle, že je pôvodcom alebo dal príčinu k bezpečnostnému incidentu.

Článok III.
Bezpečnostné opatrenia

1. Poskytovateľ nie je oprávnený pri svojej činnosti pre príjemcu akúkoľvek aktívne pristupovať k osobným údajom spracovávaných príjemcom, rovnako tak ako k informáciám o spracovaniu osobných údajov realizovaných príjemcom a ani k informáciám o zabezpečení spracovania osobných údajov.
2. Ak príde poskytovateľ pri činnosti pre príjemcov do kontaktu s osobnými údajmi, s informáciami o ich zabezpečení, či s informáciami o parametroch spracovania osobných údajov, bude o nich zachovávať mlčanlivosť. Povinnosť mlčanlivosti v potrebnej miere zaistí aj u svojich zamestnancoch a u ďalších pre neho činných osobách.
3. Pri činnosti pre príjemcov bude poskytovateľ zachovávať maximálnu šetrnosť pri nakladaní s nosičmi informácií a údajov v zmysle odst. 1. Príjemca nebude do nosičov akokoľvek zasahovať, najmä ak ide o zásahy, ktorý by mohli viesť k neoprávnenému sprístupneniu, zmene, zničeniu, zneprístupneniu, výmazu alebo poskytnutiu takých informácii alebo údajov. Uvedené platí primerane aj vo vzťahu k opatreniu a prostriedkom určeným k zabezpečeniu takých údajov a informácií.
4. Vo vzťahu k naplneniu účelu podľa odst. 1 až 3 tohoto článku prijme poskytovateľ potrebné bezpečnostné a technicko-organizačné opatrenia.
5. Súčasťou riadneho zabezpečenia a plnenia povinností podľa odst. 1 až 4 je aj pravidelné preverovanie efektivity a dostatočnosti prijatých bezpečnostných opatrení, školenie zamestnancov a osôb zapojených do činnosti pre príjemcov a overovanie ich znalostí, správneho chápania fungovania bezpečnostných pravidiel a dodržovanie stanovených opatrení a postupov.

Článok IV.
Ďalšie opatrenia k zabezpečeniu

1. Bezpečnostné opatrenia poskytovateľ uskutoční na základe riadneho zhodnotenia rizík, ich pravdepodobnosti a možných negatívnych dôsledkov z nich vyplývajúcich pre práva a slobody dotknutých osôb. Primárnym cieľom musí byť eliminovať riziká, tam kde to nie je možné potom riziká minimalizovať, a kde nie je ani to možné, eliminovať alebo aspoň minimalizovať možné negatívne dôsledky pre práva a slobody dotknutých osôb.
2. Poskytovateľ okrem iného zavedie a bude garantovať mi. tieto pravidlá a princípy určené k zaisťovaniu bezpečnosti:
   a. povinnosť počínať si tak, aby nedošlo k strate, zničeniu či neoprávnenej zmene alebo sprístupneniu údajov a informácií podľa čl. III. odst. 1 a 2. V prípade, že bezprostredne hrozí nebezpečie straty, neoprávneného zničenia, zmeny či sprístupnenia takých informácií alebo ich nosičov, povinnosť v nevyhnutnom rozsahu primeraným spôsobom zakročiť. O vykonanom zákroku, jeho dôvodoch, priebehu a dôsledkoch bez zbytočného odkladu informovať príjemcu;
   b. každý je povinný obratom správou elektronickej pošty alebo písomne spraviť určenú zodpovednú osobu o každej závade v podmienkach či jednotlivých parametroch spracovania, resp. zabezpečenia;
   c. zaistia sa aj ďalšie vhodné a potrebné bezpečnostné opatrenia, napríklad pravidelnú vynútenú zmenu prístupových hesiel;
   d. v maximálnej možnej miere využívať technických a iných možností zabezpečenia, ktorými sú zabezpečené pracovné a iné prostriedky, ktoré sa využívajú pri činnosti pre príjemcov, najmä sa zaistí povinnosť zamestnancov:
      i. uzamykanie miestností, skríň a iných priestorov, v ktorých sú uložené nosiče osobných údajov, ak nie je v priestoroch prítomný nikto oprávnený pristúpiť k predmetným osobným údajom a ich nosičom;
      ii. pri skončení práce s technickým či multimediálnym zariadením alebo aplikáciami odhlásenie z tohoto zariadenia, prostredia či aplikácie;
      iii. dôsledné utajovanie hesiel a prihlasovacích kódov pre prístup do zariadenia, multimediálneho prostredia či do jednotlivých aplikácií;
      iv. voliť bezpečné heslá, tj. heslá pozostávajúce z najmenej z 8 alfanumerických i nealfanumerických znakov, pričom každé heslo musí obsahovať veľké i malé písmená;
      v. v prípade mobilných telefónov a iných obdobných zariadení vždy zvoliť zabezpečenie pre spustenie a prihlásenie do zariadenia, rovnako ako pre jeho odomknutie, aspoň prostredníctvom zadania štvormiestneho PIN; ak je to možné, zvolí sa vždy aj vyšší spôsob zabezpečenia;
      vi. na multimediálne zariadenia a výpočtovú techniku, ktorá bola zamestnancovi zverená k plneniu pracovných úloh, bez súhlasu a asistencie zodpovednej osoby neinštalovať akýkoľvek software, či nevykonávať akékoľvek zmeny, najmä potom vyraďovať antivírusové a či iné obdobné programy určené k zaisteniu bezpečnosti spracovávaných osobných údajov;
      vii. ak je zamestnancovi zverený mobilný telefón alebo služobný PC, či iné obdobné multimediálne zariadenie či zariadenie výpočtovej techniky, najmä ak má zamestnanec možnosť disponovať s ním i mimo priestory zamestnávateľa, aby dotyčný prijal a dôsledne vykonal také opatrenia, aby úplne vylúčil prístup a dispozíciu s týmito prostriedkami zo strany akejkoľvek tretej osoby, rovnako tak ako opatrenia k tomu, aby predišiel zničeniu či poškodeniu takýchto zariadení.

Článok V.
Komunikácia

1. Komunikácia (telefónom, elektronickou poštou, bežnou poštou) súvisiace s činnosťou poskytovateľa pre príjemcu, či už je činená v rámci jednej zo strán alebo medzi nimi či voči tretím osobám (zmluvným partnerom, klientom, štátnym úradom atď.), sa realizuje vždy maximálne bezpečne a diskrétne, tj. tak, aby sa s obsahom správy, vrátane odovzdávaných informácií a údajov, nemal možnosť zoznámiť nikto iný než jej oprávnený adresát.
2. K odovzdávaniu správ obsahujúcich informácie podľa čl. III. odst. 1 a 2 slúži: dátová schránka, správa el. pošty, úložnej el. služby, alebo doručovanie prostredníctvom poskytovateľa poštových služieb, príp. iný obdobný spôsob doručovania, kedy dochádza k fyzickému odovzdaniu nosiča osobných údajov adresátovi (služby messengera atp.).
3. Ak je to s ohľadom na povahu adresáta a poskytované služby možné, použije sa ku komunikácii prednostne systém dátových schránok.
4. Ak nie je možné k odovzdaniu údajov využiť systém dátových schránok, môže využiť, ak si to vyžaduje povaha odovzdávaných informácií a ich zabezpečenie, el. poštu alebo poskytovateľa poštových služieb, príp. inú obdobnú

službu, kedy dochádza k fyzickému odovzdaniu nosiča údajov (služba messengera atp.). V týchto prípadoch je potrebné vždy určiť konkrétneho adresáta a využiť služby potvrdenia doručenia, resp. doručenia do vlastných rúk.

5. Odovzdanie informácií prostredníctvom správy el. pošty je v prípadoch podľa odst. 4 možné jedine pri riadnom zabezpečení odovzdávaných informácií. Zabezpečením sa myslí najmenšia komprimácia odovzdávaného súboru do formátu *.zip alebo podobného formátu a kódovanie predmetného súboru prostredníctvom bezpečného hesla. Bezpečným heslom sa myslí heslo najmenej o 8 znakoch, ktoré obsahuje alfanumerické (veľké aj malé písmená a číslice) i nealfanumerické znaky. Heslo musí byť s adresátom dohodnuté vopred. Heslo musí byť bezpečne odovzdané – bezpečným odovzdaním nie je odovzdanie hesla v otvorenej správe el. pošty; rovnako platí aj pre zmenu hesla.
6. Dohodnuté heslo si diskrétne povedia zodpovední zástupcovia zmluvných strán.

Článok VI.
Bezpečnostný incident

1. Ak sa poskytovateľ dozvie o bezpečnostnom incidente, je povinný ho bezodkladne oznámiť príjemcovi. Rovnaké platí aj o dôvodnom podozrení na bezpečnostný incident.
2. Predpokladom oznámenia v zmysle tohoto článku je vždy:
   a) poctivosť na strane oznamovateľa;
   b) presvedčenie oznamovateľa o pravdivosti oznámenia;
   c) presvedčenie oznamovateľa o legálnosti jednania/oznámenia;
   d) overenie oznamovaných informácií.

   Iné oznámenia (neoverené, nepoctivé – vedené úmyslom niekoho poškodiť) môžu ukladať povinnosti nahradiť ujmu (hmotnou alebo nehmotnou).
3. Bezpečnostný incident sa diskrétne oznamuje príjemcom určenej osobe.
4. Poskytovateľ zaistí, aby oznamovateľ vždy oznamoval tak, ak sa dotýka oznámenie niektorého so spoluzamestnancov alebo členov poskytovateľa alebo inej osoby, kedy taká osoba má mať postavenie porušiteľa právnych povinností, aby sa o oznámení nedozvedel oznamovaný.
5. Oznámenie sa podáva písomne alebo prostredníctvom správy el. pošty.
6. V oznámení sa uvedie (ak to bude z povahy veci možné):
   a. meno a priezvisko, pracovné zaradenie a kontaktné údaje oznamovateľa;
   b. všetko, čo o oznamovanom bezpečnostnom incidente oznamovateľa a tretej osoby vie (popis bezpečnostného incidentu);
   c. mená a priezviskách všetkých osôb, ktoré sa bezpečnostného incidentu zúčastnili, vrátame ich pracovného zaradenia alebo inštitúcie, v ktorej pôsobia a identifikácia oznamovaného;
   d. mená a priezviskách osôb, vrátane ich kontaktných údajov, ktoré majú informácie o bezpečnostnom incidente;
   e. informáciu o tom, ako a prípadne od koho sa o bezpečnostnom incidente oznamovateľ dozvedel;
   f. informáciu o tom, ako pravdivosť zistených informácií oznamovateľ a spracovateľ overili;
   g. spracovanie osobných údajov, spracovateľské operácie a osobné údaje, ktorých sa bezpečnostný incident týka, vrátane rozsahu dotknutých subjektov údajov;
   h. možné riziká, ktoré z bezpečnostného incidentu vyplávajú voči právam a slobodám subjektov údajov, správcovi, spracovateľovi alebo tretím osobám.

   K oznámeniu sa pripoja všetky dôkazné prostriedky, ktorými poskytovateľ disponuje, ktoré ich preukazujú.
7. Oznámenie sa podáva v (českom) slovenskom jazyku.