Základní škola a Mateřská škola Velemín, příspěvková organizace	
SMĚRNICE PRO GDPR	
Zpracoval:	Mgr. Ladislava Malíková
Schválil	Mgr. Ladislava Malíková
Změny ve směrnici jsou prováděny formou číslovaných písemných dodatků, které tvoří součást tohoto předpisu.	

Čl. 1
Úvodní ustanovení

1. Ředitel školy vydává tuto směrnici na základě nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob (dále jen nařízení) v souvislosti se zpracováním osobních údajů. Cílem směrnice je vytvořit ucelený soubor pravidel na ochranu osobních údajů zpracovávaných v organizaci.

2. Ředitel školy je povinen:
   - poučit zaměstnance o všech významných skutečnostech, postupech nebo událostech souvisejících s nakládáním s osobními údaji v organizaci, a to bez zbytečného odkladu;
   - zabezpečit, aby zaměstnanci organizace byli řádně informováni o právech a povinnostech při ochraně osobních údajů;
   - zařídit, aby zaměstnanci byli podle možností a potřeb správce vzděláváni nebo proškolováni o ochraně osobních údajů;
   - zajistit, aby organizace mohla řádně předložit plnění povinností při ochraně osobních údajů, které vyplývají z právních předpisů.

Čl. 2
Působnost směrnice

1. Směrnice upravuje povinnosti správce, jeho zaměstnanců, případně dalších osob při nakládání s osobními údaji, a dále pravidla pro jejich získávání, shromažďování, ukládání, použití, šíření a uchovávání.

2. Tato směrnice je závazná pro všechny zaměstnance. Všichni zaměstnanci stvrzují svým podpisem seznámení se s touto směrnicí při pravidelném ročním školení o ochraně osobních údajů.

Čl. 3
Základní pojmy

a) **Osobní údaj** je jakýkoli údaj týkající se určeného nebo určitelného subjektu údajů;

b) **Citlivý údaj** je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v politických stranách, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů;

c) **Subjekt údajů** je fyzická osoba, které se osobní údaje týkají. Osobní údaje mohou být pouze ve vztahu k žijící fyzické osobě. Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách;

d) **Zpracování osobních údajů** shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace;

e) **Pověřenec pro ochranu osobních údajů** (dále jen „pověřenec“) poskytuje informace a poradenství správci či zpracovateli, včetně zaměstnanců, kteří se na zpracování podílejí. Pověřenec monitoruje soulad zpracování s Obecným nařízením a dalšími předpisy. Pověřenec poskytuje na vyžádání poradenství, pokud jde o posouzení vlivu na ochranu osobních údajů. Nedílnou součástí výkonu funkce pověřence je dále spolupráce s Úřadem pro ochranu osobních údajů a působení jako kontaktní místo;

f) **Shromažďování osobních údajů** – je systematický postup, jehož cílem je získání osobních údajů za účelem jejich dalšího uložení na nosič informací;

g) **Likvidace osobních údajů** – rozumí se fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování;

h) **Správce osobních údajů** je každý subjekt, který určuje účely a prostředky zpracování osobních údajů, a za zpracování primárně odpovídá. Správce osobní údaje zpracovává pro účely vyplývající z jeho činnosti (např. zákonem stanovené povinnosti, ze smluv);

i) **Zpracovatel** je subjekt, který zpracovává osobní údaje pro správce. Od správce se zpracovatel liší tím, že v rámci své činnosti pro správce může provádět jen takové zpracovatelské operace, kterými jej správce pověří či vyplývají z jeho činnosti, pro kterou byl správcem pověřen;

j) **Oprávněná osoba** – je každý subjekt, který na základě pověření správcem zpracovává osobní údaje podle zákona o ochraně osobních údajů;

k) **Souhlas** subjektu údajů je jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;

l) **Anonymizace** je proces, při kterém se odstraní osobní údaje a poté nelze ani nepřímo přidělením dalších identifikátorů určit subjekt údajů;

m) **Pseudonymizace** je zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

n) **Dozorový úřad** je nezávislý orgán veřejné moci zřízený členským státem podle článku 51;

o) **Bezpečnostní událost** je událost, při které dochází k pokusu o porušení dostupnosti důvěrnosti nebo integrity u prostředků či dokumentů a která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb či bezpečnosti a integrity sítí elektronických komunikací.

p) **Bezpečnostní incident** je bezpečnostní událost, která nebyla ošetřena relevantním opatřením, a při které došlo k ohrožení bezpečnosti informací v informačních systémech, narušení bezpečnosti služeb nebo k porušení pravidel.

Čl. 4
Mlčenlivost

1. Zaměstnanci organizace se zavazují během pracovního poměru i po jeho ukončení zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví při vykonávání své činnosti.

Čl. 5
Zásady zpracování a nakládání s osobními údaji

1. Osobní údaje se mohou v organizaci zpracovávat pouze na základě právní povinnosti, životně důležitého zájmu, veřejného zájmu, oprávněného zájmu, plnění smlouvy nebo na základě souhlasu subjektu údajů.

2. Správce a jeho zaměstnanci při nakládání a zpracovávání osobních údajů aktivně spolupracují s jmenovaným pověřencem pro ochranu osobních údajů.

3. Ředitel školy důsledně zakazuje předávání osobních údajů subjektů třetím osobám soukromého práva (nabídky pomůcek, knih, aktivit pro žáky, marketingové kampaně atp.).

4. Správce a jeho zaměstnanci jsou povinni nakládat s osobními údaji v souladu s právními předpisy, a to přiměřeně, relevantně a transparentně, se zřetelem ke stanovenému účelu zpracování a výhradně v nezbytném rozsahu a dbát na to, aby zpracovávané osobní údaje byly pravdivé a přesné.

5. Osobní údaje musí být uchovány ve formě umožňující identifikaci subjektu údajů jen po nevyhnutelnou dobu.

6. Osobní údaje musí být zabezpečeny před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením prostřednictvím technických či organizačních opatření.

7. Správce uchovává osobní údaje v prostorách, na místech, v prostředí nebo v systémech, do kterých má přístup omezený, dopředu stanovený a v každý okamžik alespoň řediteli školy známý okruh osob; jiné osoby mohou nabýt přístupu k osobním údajům jedině se svolením ředitele školy nebo jím pověřené osoby.

8. Správce a jeho zaměstnanci jsou povinni dávat při zpracování zvláštní důraz na ochranu osobních údajů dětí.

9. Správce je povinen při uzavírání smluv a právních ujednání postupovat s ohledem na povinnost chránit osobní údaje před zneužitím.

10. Správce implementuje takové postupy, aby o nakládání a zpracování osobních údajů měl přehled alespoň ředitel školy nebo jím pověřená osoba a pověřenec. Mezi tyto postupy se řadí zejména tato směrnice pro ochranu osobních údajů a směrnice pro bezpečnost a nakládání s IT.

11. Správce ve spolupráci s pověřencem na ochranu osobních údajů jednou ročně provede zhodnocení postupů pro nakládání a zpracování osobních údajů. Na základě tohoto zhodnocení může správce navrhnout změny těchto postupů o nichž bude zaměstnance informovat formou školení.

Čl. 6
Zpracování zvláštních kategorií osobních údajů (citlivých údajů)

1. Zvláštní pozornost je věnována zpracování citlivých údajů. Jedná se například o údaje týkající se zdravotního stavu dítěte nebo zaměstnance školy, omezení vztahující se k poruchám učení, specifické stravovací plány související se zdravotním stavem, biometrické údaje či popis rodinného prostředí žáka.

2. Správce zpracovává tyto osobní údaje jen na základě zákonné povinnosti, v nezbytném rozsahu a dbá ve zvýšené míře o jejich zabezpečení.

3. V organizaci je zakázáno zpracovávat citlivé osobní údaje, které vypovídají o rasovém nebo etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení, dále zpracování genetických údajů a údajů o sexuálním životě nebo sexuální orientaci fyzické osoby.

4. Tyto citlivé osobní údaje je možné zpracovávat výhradně v situaci, kdy:
    - subjekt údajů udělil výslovný souhlas se zpracováním těchto údajů;
    - zpracování je nezbytné pro plnění povinností v oblasti pracovního práva, práva sociálního zabezpečení a sociální ochrany;
    - zpracování je potřebné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
    - zpracování je potřebné pro účely preventivního nebo pracovního lékařství pro posouzení pracovních schopností zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče;
    - zpracování je nutné pro účely archivace ve veřejném zájmu, pro účely vědeckého nebo historického výzkumu nebo pro statistické účely.

5. Pro zpracování citlivých osobních údajů je potřebný jednoznačný písemný souhlas v případech:

- zjištění trestní bezúhonnosti u zaměstnanců, u nichž se vyžaduje odpovědnost za svěřené hodnoty;
- pro provádění srážek ze mzdy a poukazování odborových příspěvků zaměstnanců;
- pro využití biometrických údajů v případě docházkového či přístupového systému.

Čl. 7
Organizační opatření k ochraně osobních údajů ve škole

1. Všechny listinné dokumenty obsahující osobní údaje (např. katalogové listy, třídní výkazy, a další materiály ze školní matriky) jsou nepřetržitě uschovány v uzamykatelných skříních. Třídním učitelům jsou půjčeny na nutně dlouhou dobu k provedení zápisů. Listinné dokumenty obsahující osobní údaje či jejich části nelze ze školy odnášet, předávat, nebo kopírovat a ani je jinak poskytovat neoprávněným osobám.

2. Digitální dokumenty obsahující osobní údaje jsou zpracovávány v zabezpečených informačních systémech, nebo uložené v zabezpečeném datovém úložišti. Do zmíněných informačních systémů, či datových úložišť mají přístup konkrétní zaměstnanci organizace a další osoby výhradně a písemně pověřené ředitelem školy, a to jen s využitím přiděleného přihlašovacího jména a hesla a pouze v rámci oprávnění daného funkčním zařazením.

3. Při opuštění počítače se musí zaměstnanec organizace odhlásit ze všech informačních systémů i z počítače, případně využít funkce uzamčení v operačním systému počítače. Pro zvýšení bezpečnosti je správcem sítě nastavena doba pro automatické odhlášení.

4. Zaměstnanec je zároveň povinen neumožnit nahlížení do dokumentů žádné jiné osobě a musí chránit přidělené přihlašovacího údaje a v případě nebezpečí jejich vyzrazení je okamžitě, a to ve spolupráci se správcem sítě obměnit.

5. Nastavení jednotlivých přístupů určuje ředitel školy či jím pověřený zaměstnanec a realizuje jej správce počítačové sítě, který nastavuje potřebné přístupy dle zadaných požadavků.

6. Zákonní zástupci žáků a žáci mají umožněný zabezpečený dálkový přístup pouze k vlastním záznamům o klasifikaci na základě přihlašovacího kódu a hesla předaného správcem počítačové sítě, a to přísně individuálně prostřednictvím třídních učitelů.

7. Osobní spisy zaměstnanců jsou uschovány ve zvlášť uzamykatelných skříních a přístup k nim je povolen pouze pro ředitele školy nebo zástupce ředitele, zastupuje-li ředitele, případně, je-li to potřebné též sekretářka školy nebo mzdová účetní.

8. Zaměstnanci mají právo seznámit se s obsahem svého osobního spisu.

9. Součástí osobního spisu mohou být tyto dokumenty, které jsou nutné pro výkon práce:
   - pracovní smlouva, její dodatky a mzdové nebo platové výměry;
   - pracovní povolení a povolení k pobytu;
   - podklady pro zúčtování mezd a výplatní pásky (evidence pracovní doby, DPN.);

- podklady pro plnění povinností zaměstnavatele (např. zdravotně postižení);
- zvláštní osvědčení zaměstnance (potravinářský průkaz);
- doklady o trvání a skončení pracovního poměru (vytýkací dopisy, výpovědi);
- trestní bezúhonnost zaměstnance;
- jiná výdělečná činnost zaměstnance.

10. Zpracování osobních údajů v přiměřeném rozsahu označením zaměstnanců a zveřejnění jejich pracovních kontaktních údajů je zákonné, a to i bez souhlasu zaměstnanců, protože zpracování je nevyhnutelné pro účely oprávněných zájmů zaměstnavatele či třetí strany, není-li tím narušen rozumně očekávatelný rozsah soukromí zaměstnance:
    - vhodné je vyloučení soukromých kontaktních údajů;
    - fotografie na identifikační kartě, webu nebo v propagačních materiálech však již není kontaktním údajem a je nutný souhlas zaměstnance.

11. Zaměstnanci organizace nesmějí poskytnout bez právního důvodu či pověření ředitele školy osobní údaje jiných zaměstnanců organizace a žáků cizím osobám a institucím, a to žádnou formou tedy telefonicky, SMS zprávami, emailem, poštou, internetovým přenosem, zaznamenání v listinném či digitálním dokumentu, nebo při osobním jednání.

12. Písemná hodnocení a posudky, které jsou předávány dalším subjektům na základě právní povinnosti (např. pro potřeby soudního řízení, přijímacího řízení), zpracovávají zaměstnanci pověření ředitelem školy. Nejsou nicméně oprávněni samostatně tato hodnocení podepisovat, poskytovat a odesílat jménem školy a musí zachovávat mlčenlivost o všech dotčených skutečnostech.

13. Seznamy žáků se nezveřejňují, neposkytují bez vědomého souhlasu žáků či zákonných zástupců žáků, jiným fyzickým či právnickým osobám nebo orgánům, které neplní funkci orgánu nadřízeného škole nebo nevyplývá-li to ze zákona.

14. V propagačních materiálech školy, v ročence či výroční zprávě školy, na školním webu, v tisku či na nástěnkách ve škole lze uveřejňovat textové či obrazové informace o úspěších žáků (např. u soutěží a olympiád umístění na předních místech) pouze s uvedením jména (případně ročníku či třídy) a to na základě uděleného souhlasu žáka nebo zákonného zástupce žáka. Žák nebo zákonný zástupce má právo žádat bezodkladné zablokování či odstranění informace, fotografie či záznamu žáka, který zveřejňovat nechce a udělený souhlas odvolat.

15. Fotografie a záznamy žáků či zaměstnanců školy bez uvedení jména v rámci obecné dokumentace školních akcí a úspěchů jsou školou zpracovávány na základě ustanovení §89 zákona č.89/2012 Sb., občanský zákoník za účelem obecné propagace školy. Pokud však žák, zákonný zástupce žáka či zaměstnanec nesouhlasí s pořizováním a zveřejňováním těchto fotografií či záznamů, sdělí tuto informaci řediteli školy. Ředitel školy zaznamená identifikační údaje žáka, či zaměstnance do určeného seznamu. Tento slouží jako vodítko při pořizování fotografií či jiných záznamů z těchto akcí.

16. Lékařské, psychologické a jiné průzkumy a testování mezi žáky, jejichž součástí je také uvedení osobních údajů žáka, lze uvádět jen se souhlasem žáka nebo jeho zákonného

zástupce. To neplatí u anonymních průzkumů, které nicméně musí souviset se vzděláváním na konkrétní škole a musí s ním dopředu písemně souhlasit ředitel či zástupce ředitele; to platí zejména v situaci, že výsledky jsou předávány mimo školu či zveřejňovány.

17. Pokud jsou pro správu dokumentace využívány formuláře a software, je nezbytné uskutečnit kontrolu, zda nepožadují či nenabízejí evidenci nadbytečných údajů a tyto údaje nezpracovávat.

18. Uzavírá-li škola jakoukoli smlouvu (nájemní smlouvu, smlouvu o dílo, smlouvu o poskytnutí služeb, nepojmenovanou smlouvu apod.), k jejímuž plnění je nutné druhé smluvní straně předávat osobní údaje, škola pokaždé a bezpodmínečně musí trvat na tom, aby smlouva obsahovala tyto náležitosti:
    - přesně stanovený předmět a účel zpracování;
    - kategorie osobních údajů;
    - doba zpracování;
    - rozdělení povinností správce a zpracovatele.

19. K osobním údajům mají přístup osoby k tomu oprávněné zákonem nebo na základě zákona.

20. Do jednotlivých dokumentů školy, které obsahují osobní údaje, mohou nahlížet:
    - do osobního spisu zaměstnance vedoucí pracovníci, kteří jsou zaměstnanci nadřízeni;
    - do osobního spisu zaměstnance orgány inspekce práce, úřad práce, příslušný orgán Policie České republiky, Národní bezpečnostní úřad, soud, státní zástupce, Úřad na ochranu osobních údajů, zpravodajské služby, kontrolní orgány či další příslušné orgány veřejné správy;
    - do osobního spisu zaměstnance exekutoři na základě § 33-34 exekučního řádu, kdy je zaměstnavatel povinen poskytnout spolupráci ohledně pracovních a osobních údajů dotčeného zaměstnance;
    - do osobního spisu zaměstnance samotný zaměstnanec, činit si z něho výpisky a opatřit si stejnopisy dokladů v něm obsažených, a to na náklady zaměstnavatele (§ 312 zákoníku práce);
    - do údajů žáka ve školní matrice pedagogičtí pracovníci školy (v rozsahu daném pedagogickou funkcí), sekretářka;
    - do zápisů o zdravotním stavu žáka, zpráv o vyšetření ve školním poradenském zařízení, lékařských zpráv - výchovný poradce, vedoucí pedagogičtí pracovníci, třídní učitel;
    - do spisu, vedeném ve správním řízení účastníci správního řízení, vedoucí pedagogičtí pracovníci, sekretářka, (ředitel, zástupce ředitele, vedoucí vychovatel), osoba, která je zmocněna s úředním spisem pracovat po dobu řízení.

Čl. 8
Souhlas k zpracováním osobních údajů

1. Ke zpracování osobních údajů nad rozsah vyplývající ze zákonů (ze zákona vyplývá i oprávněný zájem, plnění právní povinnosti, plnění smlouvy, veřejný zájem) je nutný souhlas osoby, o jejíž osobní údaje se jedná.

2. Souhlas musí být svobodný, poučený, konkrétní, informovaný, jasně odlišitelný (např. souhlas musí být oddělený od smlouvy nebo obchodních podmínek, nemůže být nedílnou součástí), srozumitelný, snadno přístupný a nejlépe v písemné podobě a za použití jasných a jednoduchých jazykových prostředků.

3. Souhlas se opatří výhradně pro konkrétní údaje (jasně určené např. druhově).

4. Souhlas se uděluje na konkrétní dobu (např. na celé období školní docházky na škole, na školní rok, na dobu školy v přírodě apod.) a pro konkrétní účel, který musí subjekt údajů znát.

5. Souhlas se opatří pro zpracování osobních údajů pouze tehdy, když je jejich zpracování nezbytně nutné a jiný titul není pro tento účel zpracování možný.

6. Souhlas subjektu údajů musí správce osobních údajů je povinen získat jej ještě předtím, než zpracování osobních údajů zahájí.

7. Správce je také povinen prokázat udělení souhlasu po celou dobu zpracování osobních údajů.

8. Pro subjekty údajů mladší patnácti let uděluje souhlas se zpracováním osobních údajů zákonný zástupce subjektu údajů.

9. Udělený souhlas může být v souladu s právními předpisy odvolán. Odvolání souhlasu vždy nepředstavuje pro správce povinnost osobní údaje zlikvidovat, ale představuje pro správce pouze povinnost přestat osobní údaje zpracovávat pro určitý účel, ke kterému byl souhlas udělen. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

Čl. 9
Bezpečnost informací

1. Zabezpečení listinných dokumentů a záznamových médií obsahujících osobní údaje:
    - dokumenty a záznamová média, která obsahují osobní údaje, musí být zabezpečeny v uzamčených skříních, případně na jiných místech, kde je možné zajistit jejich ochranu;
    - to platí také pro kopie dokumentů obsahující osobní údaje;
    - k dokumentům a záznamovým médiím, které obsahují osobní údaje, nesmí mít přístup neoprávněné osoby;

- dokumenty ani záznamová média nesmí zůstat bez dohledu na stolech pracovníků. Pokud, zaměstnanec odejde od svého pracovního místa, musí dané dokumenty a záznamová média řádně zabezpečit (např. zamknout celou kancelář, kam má přístup jen daný pracovník či uschovat dokumenty a záznamová média do uzamykatelné skříně, nebo šuplíku, dokumenty na tiskovém zařízení, ke kterému má přístup více lidí, se musí okamžitě odebírat a nesmí se nechávat bez dozoru atd.).

2. Zabezpečení digitálních dokumentů a dat obsahujících osobní údaje:
   - dokumenty obsahující osobní údaje, které jsou uloženy v digitálních zařízeních či síťových úložištích, musí být zabezpečeny před přístupem neoprávněných osob, ztrátou, zničením, před změnou, neoprávněným přenosem, jiným neoprávněným zpracováním, jakož i jiným zneužitím;
   - přístupy k těmto dokumentům, prováděné operace a jejich předávání je monitorováno prostřednictvím bezpečnostních evidenčních záznamů;
   - data informačních systémů, počítačové databáze či digitální dokumenty jsou uchovány na zabezpečeném úložišti školního serveru či v zabezpečeném cloudovém úložišti;
   - přihlašovací údaje musí být zabezpečeny silným heslem (alespoň 8 znaků, kombinace malých a velkých písmen, číslic a zvláštních znaků) a nesmí být předávány žádným dalším osobám včetně vedení školy;
   - výjimkou je předání přístupových údajů správci sítě pro nutný případ servisního zásahu, po tomto úkonu je však uživatel povinen své heslo bezprostředně změnit.

Čl. 10
Práva subjektu údajů

1. Oznámení správce subjektu údajů o tom, že jsou zpracovávány jeho osobní údaje, musí být uskutečněno nejdéle ve chvíli jejich shromáždění od subjektu údajů.

2. V případě, kdy dochází k předávání osobních údajů, informuje správce osobních údajů v dokumentu Zásady ochrany osobních údajů, který je umístěn na webových stránkách správce.

3. Pokud se správce chystá zpracovat osobní údaje pro jiný účel, než je účel, pro který byly shromážděny, musí poskytnout subjektu údajů informace o tomto jiném účelu a další nezbytné informace ještě před uvedeným dalším zpracováním.

4. Pokud se osobní údaje týkající se subjektu získávají od subjektu samotného, poskytne správce v okamžiku získání těchto osobních údajů tyto informace:
   - totožnost a kontaktní údaje správce a jeho případného zástupce;
   - kontaktní údaje pověřence pro ochranu osobních údajů;
   - účel zpracování, pro který jsou osobní údaje určeny, a právní titul pro toto zpracování;
   - případné příjemce nebo kategorie příjemců osobních údajů;
   - potenciální úmysl správce svěřit osobní údaje do třetí země nebo mezinárodní organizaci;

- doba, po kterou budou osobní údaje uchovány, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
- existence práva žádat od správce přístup k osobním údajům týkajícím se subjektu, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
- existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
- existence práva podat stížnost u dozorového úřadu.

Čl. 11
Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu

1. Správce řeší okamžitě každou bezpečnostní událost týkající se osobních údajů, a to ve spolupráci s pověřencem pro ochranu osobních údajů a správcem počítačové sítě.

2. V situaci, kdy je při šetření bezpečnostní události patrné, že konkrétní případ porušení zabezpečení osobních údajů bude mít za následek veliké riziko pro práva a svobody fyzických osob jedná se o bezpečnostní incident.

3. Bezpečnostní incident správce v prvé řadě a bez zbytečného odkladu nahlásí dotčenému subjektu údajů.

4. V oznámení určeném subjektu údajů se za použití přesných a jednoduchých jazykových nástrojů popíše povaha porušení zabezpečení osobních údajů a uvedou se v něm přinejmenším informace a opatření uvedené v čl. 33 odst. 3 písm. b), c) a d).

5. Oznámení subjektu údajů nemusí být, je-li splněna kterákoli z těchto podmínek:
   - správce zahájil příslušná technická a organizační ochranná opatření a tato opatření byla využita u osobních údajů dotčených předmětným porušením zabezpečení osobních údajů, zvláště taková, která dělají tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování;
   - správce nastavil následná opatření, která zabezpečí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 2 se již podle všeho neprojeví;
   - vyžadovalo by to nepoměrné úsilí. V takové situaci musí být subjekty údajů poučeny stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

6. Pokud správce dotčenému subjektu údajů porušení zabezpečení osobních údajů doposud neohlásil, může dozorový úřad po posouzení pravděpodobnosti toho, že dané porušení bude mít za následek veliké riziko, žádat, aby tak udělal.

7. O každém bezpečnostním incidentu se učiní zápis, který provede pověřenec do registru bezpečnostních incidentů a zároveň uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření.

8. Každý bezpečnostní incident oznamuje pověřenec dozorovému úřadu dle článku 33 nařízení, a to bez zbytečného odkladu a nejdéle do 72 hodin od chvíle, kdy se o něm

dozvěděl. Pokud nebude ohlášení dozorovému úřadu učiněno do 72 hodin, musí být zároveň s ním uvedeny důvody tohoto zpoždění.

9. Ohlášení musí obsahovat alespoň:
    - určení povahy daného případu porušení zabezpečení osobních údajů včetně, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
    - jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
    - popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
    - popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.