Číslo dokumentu:	SOP-529	Název:	Platnost od:	15.7.2018
Vydání číslo: 1	Výtisk číslo: 1	**Směrnice OCHRANA OSOBNÍCH ÚDAJŮ**	Počet stran:	34

Zpracoval:	Ověřil:	Schválil:
Jméno a příjmení: **Ing. David Zahradnický** Datum: 14.7.2018 Podpis:	Jméno a příjmení: **Mgr. Veronika Králíková** Datum: 14.7.2018 Podpis:	Jméno a příjmení: **Bc. Viktor Furman, MBA.** Datum: 15.7.2018 Podpis:

Č. revize	Jméno osoby provádějící revizi/změnu	Výsledek revize / Změna číslo XX na listech č. XX	Datum/ podpis	Změnu schválil
1.				
2.				
3.				
4.				
5.				

Č. revize	Jméno osoby provádějící revizi/změnu	Výsledek revize / Změna číslo XX na listech č. XX	Datum/ podpis	Změnu schválil
6.				
7.				
8.				
9.				
10.				
11.				
12.				

Název SOP

Směrnice OCHRANA OSOBNÍCH ÚDAJŮ

Účel

Směrnice je řízeným dokumentem společnosti GHC GENETICS, s.r.o. (dále také GHC nebo organizace nebo společnost) a je jejím duševním majetkem. Předávání kopií tohoto dokumentu mimo organizaci je možné pouze se souhlasem jednatele. Vyplněný změnový list je uložen u MANAŽEAR KVALITY.

OBSAH

ÚVOD

1.1. Účel

Směrnice je vydaná dle nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Dále jen „Nařízení".
Účelem je stanovit prostředky a způsob zpracování osobních údajů a zajistit ochranu osobních údajů ve společnosti GHC GENETICS, s.r.o.

1.2. Oblast platnosti

Směrnice má platnost v celé společnosti a je závazná pro všechny pracovníky.

I.DEFINICE A ZKRATKY

Osobní údaj	veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby
Subjekt údajů	fyzická osoba, k níž se osobní údaje vztahují
Zpracování	jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení
Omezení zpracování	označení uložených osobních údajů za účelem omezení jejich zpracování v budoucnu
Profilování	jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu
Pseudonymizace	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
Správce (osobních údajů)	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a

	prostředky zpracování osobních údajů
Společní správci (osobních údajů)	pokud účely a prostředky zpracování stanoví společně dva nebo více správců, jsou společnými správci.
Zpracovatel (osobních údajů)	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
Příjemce (osobních údajů)	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
Třetí strana	fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů
Souhlas (subjektu údajů)	jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů;
Zvláštní údaj	osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.
Anonymní informace	údaj, který buď v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určenému nebo určitelnému subjektu údajů. Míra anonymizace může být částečná nebo úplná. Za zcela anonymní údaj lze považovat takový údaj, u něhož není možné nadále určit subjekt údaje, tzn. že jej nelze vztáhnout ke konkrétní fyzické osobě a neobsahuje žádnou charakteristiku či jedinečný znak této fyzické osoby. Nařízení se na tato data nevztahuje.

ÚOOÚ	Úřad pro ochranu osobních údajů
OÚ	Osobní údaj
EU	Evropská unie
SÚ	Subjekt údajů
GDPR	General Data Protection Regulation

II.Působnost Nařízení o ochraně osobních údajů

(1) Nařízení se vztahuje na:

- na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.
- zpracování osobních údajů v souvislosti s činnostmi provozovny správce nebo zpracovatele v EU bez ohledu na to, zda zpracování probíhá v EU nebo mimo ni

(2) Nařízení se nevztahuje na zpracování osobních údajů prováděné:

- při výkonu činností, které nespadají do oblasti působnosti práva EU
- fyzickou osobou v průběhu výlučně osobních či domácích činností

- příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

III.ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Osobní údaje musí být:

- ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);
- shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný; další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely se nepovažuje za neslučitelné s původními účely („účelové omezení“);
- přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);
- přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny („přesnost“);
- uloženy ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány; osobní údaje lze uložit po delší dobu, pokud se zpracovávají výhradně pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely, a to za předpokladu provedení příslušných technických a organizačních opatření s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);
- zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením („integrita a důvěrnost“);

IV.ZÁKLADNÍ USTANOVENÍ

(1) Společnost GHC je správcem a zároveň zpracovatelem osobních údajů ve smyslu Nařízení.

(2) Společnost GHC odpovídá za dodržení výše uvedených zásad a musí být schopen toto dodržení souladu doložit („odpovědnost“). Za zajištění odpovídají příslušní vedoucí úseků.

(3) Ke zpracování osobních údajů může společnost GHC uzavřít smlouvu o zpracování osobních údajů se Zpracovatelem. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá. Zpracovatel musí ve smlouvě poskytnout dostatečné záruky o technickém a organizačním zabezpečení ochrany osobních údajů. Na zpracovatele se vztahují stejné povinnosti jako na správce s ohledem na skutečnost, že může mít přístup k osobním údajům ve stejném rozsahu jako správce.

(4) Společnost GHC je povinna provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány.

(5) Porušení povinností zaměstnance při ochraně osobních údajů je posuzováno jako porušení pracovní kázně.

(6) Společnost GHC nakládá s osobními údaji zákonným způsobem, pokud:

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

(7) Zakazuje se zpracování zvláštních osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby, s výjimkou že:

- subjekt údajů udělil výslovný souhlas se zpracováním těchto osobních údajů pro jeden nebo více stanovených účelů,
- zpracování je nezbytné pro účely plnění povinností a výkon zvláštních práv správce nebo subjektu údajů v oblasti pracovního práva a práva v oblasti sociálního zabezpečení a sociální ochrany
- zpracování je nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby v případě, že subjekt údajů není fyzicky nebo právně způsobilý udělit souhlas;
- zpracování provádí v rámci svých oprávněných činností a s vhodnými zárukami nadace, sdružení nebo jiný neziskový subjekt, který sleduje politické, filozofické, náboženské nebo odborové cíle, a za podmínky, že se zpracování vztahuje pouze na současné nebo bývalé členy tohoto subjektu nebo na osoby, které s ním udržují pravidelné styky související s jeho cíli, a že tyto osobní údaje nejsou bez souhlasu subjektu údajů zpřístupňovány mimo tento subjekt;
- zpracování se týká osobních údajů zjevně zveřejněných subjektem údajů;
- zpracování je nezbytné pro určení, výkon nebo obhajobu právních nároků nebo pokud soudy jednají v rámci svých soudních pravomocí;
- zpracování je nezbytné z důvodu významného veřejného zájmu na základě práva EU nebo členského státu, které je přiměřené sledovanému cíli, dodržuje podstatu práva na ochranu údajů a poskytuje vhodné a konkrétní záruky pro ochranu základních práv a zájmů subjektu údajů;
- zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče
- zpracování je nezbytné z důvodů veřejného zájmu v oblasti veřejného zdraví, jako je ochrana před vážnými přeshraničními zdravotními hrozbami nebo zajištění přísných norem kvality a bezpečnosti zdravotní péče a léčivých přípravků nebo zdravotnických prostředků.

V.ÚČEL ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

(1) Společnost GHC provádí shromažďování a zpracování osobních údajů fyzických osob v rozsahu potřebném:

- k plnění povinností uložených zvláštním zákonem,
- k zajišťování činností spojených s předmětem podnikání,
- k jednání o smluvním vztahu,
- k plnění smlouvy uzavřené se subjektem údajů,
- k nabízení obchodu nebo služeb subjektům údajů,
- v rámci agendy společníků společnosti,
- k zajištění ochrany majetku a bezpečnosti práce

(2) Podrobné rozepsání účelu zpracování osobních údajů je uvedeno v analýze osobních údajů nebo v záznamech o zpracování.

VI.ZDROJE ZÍSKÁVÁNÍ OSOBNÍCH ÚDAJŮ

(1) Společnost GHC získává osobní údaje ze zdrojů:

- přímo od fyzických osob při jednání o smluvním vztahu
- od pacientů odebráním vzorku nesoucí genetické informace
- z veřejně přístupných rejstříků, seznamů a evidencí (např. Obchodní rejstřík, Živnostenský rejstřík, Katastr nemovitostí, veřejný telefonní seznam apod.).
- od dalších subjektů, pokud tak stanoví zvláštní předpis.
- od dalších subjektů, pokud k tomu dala fyzická osoba svůj souhlas.
- Při přijímacích řízeních nových zaměstnanců

VII.PRÁVA SUBJEKTU ÚDAJŮ

8.1. Souhlas se zpracováním osobních údajů

(1) Pokud je zpracování založeno na souhlasu, musí být správce schopen tento souhlas doložit (viz formulář GDPR_F-06, GDPR_F-07, GDPR_F-08). Souhlas musí být od jiných skutečností jasně odlišitelný, srozumitelný a snadno přístupný za použití jasných a jednoduchých jazykových prostředků. Souhlas musí být svobodný, konkrétní, informovaný a jednoznačný

(2) Musí z něj být patrno:

- v jakém rozsahu je poskytován (tj. jaké osobní údaje mohou být zpracovány),
- komu je poskytován (tj. jakému správci: oficiální název organizace, adresa jejího sídla, možnost písemného nebo elektronického kontaktu),
- k jakému účelu (tj. pro který konkrétní účel zpracování),
- na jaké období a kdo jej poskytuje (tj. určení časového období, na které je souhlas dáván, a identifikace toho, kdo souhlas poskytuje).
- souhlas se zpracováním osobních údajů musí společnost GHC prokázat po celou dobu zpracování osobních údajů, k jejichž zpracování byl poskytnut.

(3) Subjekt údajů má právo svůj souhlas kdykoli odvolat. Odvoláním souhlasu není dotčena zákonnost zpracování vycházejícího ze souhlasu, který byl dán před jeho odvoláním. Před udělením souhlasu o tom bude subjekt údajů informován. Odvolat souhlas musí být stejně snadné jako jej poskytnout.

(4) Pokud se ve společnosti nakládá s osobními údaji dětí do věku 15 let, musí být souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti.

(5) Souhlas subjektu údajů nemůže legitimizovat zpracování osobních údajů, které je svou podstatou protiprávní. Na správce a zpracovatele se vztahují příslušná ustanovení Nařízení a jejich nedodržení nelze nahradit souhlasem subjektu údajů.

(6) Bez tohoto souhlasu je může společnost GHC zpracovávat, pokud:

- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce
- zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

8.2. Právo na přístup k osobním údajům

(1) Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím:
- účely zpracování;
- kategorie dotčených osobních údajů;
- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích;
- plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
- existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;
- právo podat stížnost u dozorového úřadu;
- veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
- skutečnost, že dochází k automatizovanému rozhodování, včetně profilování,

(2) Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách, které se vztahují na předání.

(3) Správce poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.

(4) Požadavky na zajištění práva na přístup k osobním údajům:
- je zajištěn přístup subjektu údajů k informacím o zpracování osobních údajů a k osobním údajům o účelech zpracování, o kategoriích osobních údajů, o příjemcích nebo kategoriích příjemců i ve třetích zemích, o době uchování, nebo kritériích, podle nichž bude doba stanovena, o právech subjektů údajů (na opravu údajů, na výmaz údajů, na omezení zpracování, na námitku proti zpracování, na podání stížnosti u dozorového úřadu), veškeré dostupné informace o zdroji údajů (pokud jím není přímo subjekt údajů), že dochází k automatizovanému rozhodování, včetně profilování při zpracování osobních údajů (postup zpracování, význam zpracování, důsledky zpracování), v případě předání do třetích zemí nebo mezinárodní organizaci o vhodných zárukách, které se vztahují k předání.
- správce vydává potvrzení subjektu údajů, že osobní údaje o něm jsou nebo nejsou zpracovávány a je zajištěn přístup subjektu údajů k jeho osobním údajům.

Údaje jsou poskytovány subjektu údajů jsou podávány tak, že nedochází k dotčení práva svobod jiných osob.

8.3. Právo na opravu

(1) Subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se ho týkají. S přihlédnutím k účelům zpracování má subjekt údajů právo na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.

(2) Požadavky na zajištění práva na opravu:
- Správce přijímá žádosti subjektu údaje o opravu nepřesných údajů, opravuje bez zbytečného odkladu nepřesné osobní údaje, přijímá žádosti subjektu údaje o doplnění neúplných údajů (i dodatečným prohlášením), doplňuje bez zbytečného odkladu neúplné údaje. Správce oznamuje jednotlivým příjemcům údajů veškeré opravy osobních údajů s výjimkou případů, kdy se to ukáže jako nemožné nebo kdy to vyžaduje nepřeměřené úsilí. V případě žádosti subjektů údajů správce informuje subjekt údajů o tom, kterým příjemců zaslal oznámení o opravách osobních údajů.

8.4. Právo na výmaz (právo „být zapomenut“)

(1) Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:
- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;
- subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány, a neexistuje žádný další právní důvod pro zpracování;
- subjekt údajů vznese námitky proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování, protože osobní údaje byly zpracovány protiprávně;
- osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu EU nebo členského státu, které se na správce vztahuje;

(2) Výmaz se neuplatní, pokud je zpracování nezbytné:
- pro výkon práva na svobodu projevu a informace;
- pro splnění právní povinnosti, jež vyžaduje zpracování podle práva Unie nebo členského státu, které se na správce vztahuje, nebo pro splnění úkolu provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
- z důvodů veřejného zájmu v oblasti veřejného zdraví v
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely, pokud je pravděpodobné, že by právo uvedené v odstavci 1 znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;
- pro určení, výkon nebo obhajobu právních nároků.

(3) Požadavky na zajištění práva na výmaz:
- Správce přijímá žádosti o výmaz osobních údajů od subjektu údajů a vymaže osobní údaje, pokud zpracování nepodléhá výjimce dle bodu 2. Pokud údaje byly zveřejněny, přijímá správce (s ohledem na dostupnou technologii a náklady) přiměřené kroky, aby informoval správce, kteří údaje také zpracovávají, že je subjekt údajů žádá, aby vymazaly veškeré kopie, replikace a odkazy na tyto údaje. Správce příjemcům údajů oznamuje výmaz osobních údajů, s výjimkou případů, kdy se to ukáže jako nemožné nebo kdy to vyžaduje nepřeměřené úsilí. V případě žádosti subjektů údajů správce informuje subjekt údajů o tom, kterým příjemců zaslal oznámení o výmazu osobních údajů.

8.5. Právo na omezení zpracování

(1) Subjekt údajů má právo na to, aby správce omezil zpracování, v kterémkoli z těchto případů:
- subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
- zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
- správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
- subjekt údajů vznesl námitku proti zpracování, dokud nebude ověřeno, zda oprávněné důvody správce převažují nad oprávněnými důvody subjektu údajů.

(2) Požadavky na zajištění práva na omezení zpracování:
- Správce přijímá žádost subjektu údajů o omezení zpracování jeho osobních údajů, omezí zpracování osobních údajů, pokud zpracování podléhá situacím uvedených v bodě 1. Pokud došlo k omezení zpracování údajů, osobní údaje mohou být zpracovávány pouze se souhlasem subjektu údajů, s výjimkou uložení osobních údajů. Správce oznamuje jednotlivým příjemcům osobních údajů omezení zpracování osobních údajů s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřeměřené úsilí.

- V případě žádosti subjektů údajů správce informuje subjekt údajů o tom, kterým příjemcům zaslal oznámení o omezení zpracování osobních údajů. Správce musí ověřit přesnost osobních údajů v případě, že ji subjekt popírá a pokud dochází ke zrušení omezení zpracování, musí na to být upozorněn subjekt údajů (který dosáhl omezení).

8.6. Právo na přenositelnost údajů

(1) Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:
- zpracování je založeno na souhlasu se zpracováním osobních údajů
- zpracování se provádí automatizovaně

(2) Požadavky na zajištění práva na přenositelnost údajů:
- Správce přijímá žádost subjektu údajů o zajištění o přenositelnosti jeho údajů a zajistí přenositelnost osobních údajů, pokud zpracování podléhá situacím uvedených v bodě 1. Pokud je to technicky proveditelné, osobní údaje poskytuje jeden správce přímo druhému správci. Správce osobní údaje subjektů údajů poskytuje a/nebo přijímá v požadovaném formátu, který je strukturovaný, strojově čitelný, běžný. Uplatněním práva není dotčeno právo na výmaz údajů a nejsou nepříznivě dotčena práva a svobody jiných subjektů.

8.7. Právo vznést námitku

(1) Subjekt údajů má právo kdykoli vznést námitku proti zpracování osobních údajů, které se jej týkají. Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.

(2) Pokud se osobní údaje zpracovávají pro účely přímého marketingu, má subjekt údajů právo vznést kdykoli námitku proti zpracování osobních údajů, které se ho týkají, pro tento marketing.

(3) Pokud subjekt údajů vznese námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.

(4) Subjekt údajů je na právo výslovně upozorněn a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.

(5) Požadavky na zajištění práva vznést námitku:
- Správce přijímá dokumenty o vznesení námitky subjektu údajů proti zpracování jeho osobních údajů, vyřizuje námitky a o způsobu vyřízení informuje subjekt údajů.
- Je zajištěno, v případě využívání služeb informační společnosti, že subjekt údajů může uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací

8.8. Automatizované individuální rozhodování, včetně profilování

(1) Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.

(2) Výjimkou je, pokud je rozhodnutí:
- nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů;
- nebo povoleno právem EU nebo členského státu, které se na správce vztahuje a které rovněž stanoví vhodná opatření zajišťující ochranu práv a svobod a oprávněných zájmů subjektu údajů;
- nebo založeno na výslovném souhlasu subjektu údajů.

(3) Požadavky na zajištění práva nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování (včetně profilování):
- Správce přijímá žádosti subjektu údajů nebýt předmětem rozhodnutí založeného výhradně na automatizovaném zpracování a na žádost subjektu údajů ukončí provádění rozhodování

založeného výhradně na automatizovaném zpracování, pokud rozhodování nepodléhá výjimce dle bodu 2.

- Správce musí provést vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektů údajů minimálně v rozsahu práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.
- V případech, kdy jsou zpracovávány zvláštní kategorie osobních údajů, a zároveň je rozhodnutí nezbytné k uzavření nebo plnění smlouvy se subjektem údajů, nebo je rozhodnutí povoleno právem EU nebo ČR (včetně právem stanovených opatření zajišťujících ochranu práv a svobod), nebo je rozhodnutí založeno na výslovném souhlasu subjektu údajů, musí jít o zpracování, kde jsou zavedena vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů.
- A zároveň je zpracování nezbytné z důvodu veřejného zájmu na základě práva EU nebo ČR, který je přiměřený sledovanému cíli, dodržuje podstatu práva na ochranu osobních údajů nebo poskytuje vhodné a konkrétní záruky pro ochranu lidských práv a zájmů subjektu údajů. Nebo pokud je založené na výslovném souhlasu subjektu údajů (netýká se případů, kdy právo EU nebo ČR stanoví, že výslovný souhlas nelze uplatnit)

8.9. Údaje poskytované subjektu údajů během uplatňování práv

(1) Bez zbytečného odkladu, nejpozději do jednoho měsíce po obdržení žádosti (s ohledem na složitost a počet případů lze lhůtu prodloužit ještě o další dva měsíce a o každém prodloužení lhůty je subjekt informován včetně důvodů prodloužení).
(2) Pokud má správce pochybnosti o totožnosti osoby, která podává žádost, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů.
(3) Pokud subjekt údajů podá žádost v elektronické podobě a nepožaduje odpověď v jiné podobě, poskytuje správce informace v běžně používané elektronické podobě.
(4) Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně, nejpozději do jednoho měsíce subjekt údajů o důvodech nepřijetí žádosti, o možnosti podat stížnost u dozorového orgánu a žádat soudní ochranu.
(5) Informace je podávána bezplatně s výjimkou nedůvodných a nepřiměřených (zejména opakovaných) žádostí, kdy správce může odmítnout žádosti vyhovět nebo může požadovat přiměřený poplatek s ohledem administrativní náklady spojené s poskytnutím informace. Správce dokládá nedůvodnost nebo nepřiměřenost žádosti.

VIII. POVINNOSTI SPRÁVCE

9.1. Obecné povinnosti

(1) S přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k rizikům pro práva a svobody fyzických osob zavede správce vhodná technická a organizační opatření (viz kap.12), aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s Nařízením. Tato opatření musí být podle potřeby revidována a aktualizována.
(2) Správce rovněž zajistí výkon práv subjektu údajů.
(3) Správce je povinen dodržovat zásady nakládání s osobními údaji (viz kap.12).
(4) Citlivé údaje zpracovávat pouze pracovníky/subjekty vázaným služebním tajemstvím nebo na jeho odpovědnost, zavázat tyto pracovníky/subjekty povinností mlčenlivosti.
(5) Společní správci mezi sebou transparentním ujednáním vymezí své podíly na odpovědnosti za plnění povinností, zejména pokud jde o výkon práv subjektu údajů, a své povinnosti poskytovat informace. Bez ohledu na podmínky ujednání může subjekt údajů vykonávat svá práva podle tohoto nařízení u každého ze správců i vůči každému z nich.

9.2. Informace o zpracování osobních údajů

(1) V okamžiku získání osobních údajů správce poskytne informace subjektu údajů o nakládání s osobními údaji (viz formulář GDPR_F-04, GDPR_F-05).

(2) V případě, že osobní údaje nebyly získány od subjektu údajů, správce musí poskytnout informace subjektu údajů, pokud je to možné a nevyžaduje to nepřiměřené úsilí (viz formulář GDPR_F-04, GDPR_F-05)
- v přiměřené lhůtě po získání osobních údajů, ale nejpozději do jednoho měsíce, s ohledem na konkrétní okolnosti, za nichž jsou osobní údaje zpracovávány;
- nebo nejpozději v okamžiku, kdy poprvé dojde ke komunikaci se subjektem údajů, mají-li být osobní údaje použity pro účely této komunikace;
- nebo nejpozději při prvním zpřístupnění osobních údajů, pokud je má v úmyslu zpřístupnit jinému příjemci.

(3) Pokud správce hodlá osobní údaje dále zpracovat pro jiný účel, než pro který byly získány, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace, pokud je to možné a nevyžaduje to nepřiměřené úsilí, o tomto jiném účelu a příslušné další informace.

(4) Správce musí jednotlivým příjemcům osobních údajů oznámit všechny opravy, výmazy, doplnění nebo omezení zpracování, pokud je to možné a nevyžaduje to nepřiměřené úsilí.

9.3. Záznamy o činnostech zpracování

(1) Správce musí vést záznamy o zpracování (viz Analýza OÚ, popř. formulář GDPR_F-03), pokud společnost má více než 250 zaměstnanců nebo zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů uvedených nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

(2) Tyto záznamy poskytne správce na požádání dozorovému úřadu.

9.4. Porušení zabezpečení osobních údajů

(1) Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob. Viz formulář GDPR_F-01.

(2) Správce dokumentuje veškeré případy porušení zabezpečení osobních údajů, přičemž uvede skutečnosti, které se týkají daného porušení, jeho účinky a přijatá nápravná opatření. Tato dokumentace musí dozorovému úřadu umožnit ověření souladu s Nařízením.

(3) Pokud je pravděpodobné, že určitý případ porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob, oznámí správce toto porušení bez zbytečného odkladu subjektu údajů. Viz formulář GDPR_F-02. Oznámení subjektu údajů uvedené se nevyžaduje, je-li splněna kterákoli z těchto podmínek:
- správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými, jako je například šifrování;
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví;
- vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

9.5. Posouzení vlivu na ochranu osobních údajů a předchozí konzultace

(1) Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

(2) Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů, byl-li jmenován. Nebyl-li jmenován, je možná konzultace s pracovníkem externí poradenské společnosti.

(3) Posouzení vlivu na ochranu osobních údajů je nutné zejména v těchto případech:

- systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
- rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů; nebo
- rozsáhlé systematické monitorování veřejně přístupných prostorů.

(4) Správce provede přezkum s cílem posoudit, zda je zpracování prováděno v souladu s posouzením vlivu na ochranu osobních údajů alespoň v případech, kdy dojde ke změně rizika, jež představují operace zpracování.

(5) Správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.

9.6. Pověřenec pro ochranu osobních údajů

(1) Správce jmenuje pověřence pro ochranu osobních údajů v každém případě, kdy:
- zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
- hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo
- hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů

(2) Společnost GHC jmenuje Pověřence pro ochranu osobních údajů (DPO) jelikož ve velkém rozsahu zpracovává zvláštní kategorie osobních údajů, konkrétně biologické vzorky a lékařskou dokumentaci a tím související.

9.7. Společní správci

(1) Společní správci mezi sebou transparentním ujednáním vymezí své podíly na odpovědnosti za plnění povinností, zejména pokud jde o výkon práv subjektu údajů, a své povinnosti poskytovat informace. V ujednání může být určeno kontaktní místo pro subjekty údajů.

(2) Subjekt údajů musí být o podstatných prvcích ujednání informován.

(3) Subjekt údajů může vykonávat svá práva podle tohoto nařízení u každého ze správců i vůči každému z nich.

IX. POVINNOSTI ZPRACOVATELE

(1) Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.

(2) Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:
- zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu;
- zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;
- dodržuje podmínky pro zapojení dalšího zpracovatele

- zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů;
- je správci nápomocen při zajišťování souladu s povinnostmi, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;
- v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo EU nebo členského státu nepožaduje uložení daných osobních údajů;
- poskytne správci veškeré potřebné informace.

(3) Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření.

(4) Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

(5) Jmenuje pověřence a zajistí další činnosti stejně jak správce v kap. 9.6.

X. ANALÝZA OSOBNÍCH ÚDAJŮ A SOUVISEJÍCÍCH RIZIK

11.1. Identifikace, kategorizace, účel, místo a doba zpracování osobních údajů

(1) Pro účely stanovení povinností vyplývajících z Nařízení a stanovení organizačních a technických opatření v oblasti ochrany osobních údajů společnost GHC zpracovává analýzu osobních údajů, kde je uvedeno pro každý osobní údaj fyzických osob (partneři, zákazníci, dodavatelé, zaměstnanci a další dotčené osoby):

- uložení
- druh OÚ
- kategorie OÚ
- typ dokumentu
- účel zpracování
- právní základ pro zpracování
- odpovědnost za zpracování
- míra rizika (dále viz. kap. 11.2.)
- technická opatření
- organizační opatření
- doporučená řešení

(2) Údaje uvedené v analýze jsou předmětem pravidelného přezkoumávání a aktualizace minimálně 1x za rok a dále při zjištění slabého místa v zabezpečení osobních údajů, při změně bezpečnostních požadavků, při bezpečnostním incidentu nebo změny v relevantních osobních údajích či hrozeb. V podmínkách společnosti odpovídá MANAŽER KVALITY.

(3) V případě stanovení pověřence pro ochranu osobních údajů je tato analýza projednávána s pověřencem.

11.2. Hodnocení a řízení rizik

11.2.1. Identifikace hrozeb, zranitelných míst a následků.

(1) Hrozba je potenciální příčina porušení zabezpečení osobních údajů, která může mít za následek poškození práva svobod fyzických osob.

(2) Hrozby mohou mít charakter lidského selhání (např. odposlechy, ztráty listin, hacking informačního systému, krádež, chyby a opomenutí, vymazání souborů, nesprávné směrování emailů,..) nebo fyzického a technického prostředí (zemětřesení, blesk, požár, povodeň, zastaralý HW, výpadky el. energie, přetížení sítě, elektromagnetická radiace, ….).
(3) Zranitelné místo je slabina využitelná k uskutečnění konkrétní hrozby ve vztahu k ochraně osobních údajů.
(4) Zranitelná místa jsou důsledkem opomenutí nebo zanedbání některých aspektů nebo požadavků při řešení projektu ochrany osobních údajů:

a) v návrhu projektu ochrany osobních údajů:
- ve specifikaci požadavků na technickou bezpečnost,
- ve specifikaci požadavků na administrativní bezpečnost,
- ve specifikaci požadavků na bezpečnost informačních systémů.

b) při realizaci projektu ochrany osobních údajů:
- nedodržení specifikace požadavků na technickou bezpečnost,
- nedodržení specifikace požadavků na administrativní bezpečnost,
- nedodržení specifikace požadavků na bezpečnost informačních systémů.

c) po zahájení zpracování osobních údajů:
- zaměstnanci určení pro zpracování osobních údajů,
- nepovolané osoby,
- nedostatečné uplatňování opatření stanovených pro oblast personální bezpečnosti,
- nedodržování opatření stanovených pro administrativní bezpečnost,
- nedodržování stanoveného způsobu technické bezpečnosti,
- nedodržování stanoveného způsobu informační bezpečnosti,
- neodstraňování zjištěných závad,
- neprovádění stanovené kontrolní činnosti.

(5) Následek určuje míru škod způsobených subjektu údajů při úniku či zneužití osobních údajů.

11.2.2. Riziko ochrany osobních údajů obecně

(1) Riziko je potenciální možnost, že daná hrozba využije zranitelnosti osobních údajů nebo skupiny osobních údajů a způsobí tak únik, poškození nebo ztrátu a s následkem poškození práva svobod fyzických osob.
(2) Míra rizika je stanovena součinem tří parametrů – Hrozba, Zranitelnost, Následek. Čím vyšší výsledek, tím vyšší míra rizika. Konkrétní informace pro výpočet míry rizika je jsou uvedeny přímo v Analýze rizik (viz Analýza OÚ, sheet Analýza rizik).
(3) Rizika jsou určována v rámci analýzy osobních údajů. Odpovídá MANAŽER KVALITY.
(4) Pokud riziko významně ovlivní práva a svobody fyzických osob, je toto riziko považováno za vysoké a tato skutečnost je zaznamenána do analýzy údajů a následuje plnění dalších povinností ze strany společnosti GHC (zajištění Posouzení vlivu na ochranu osobních údajů, předchozí konzultace na příslušném dozorovém úřadu, hlášení porušení zabezpečení osobních údajů).
(5) Analýza rizik je předmětem pravidelného přezkoumávání a aktualizace minimálně 1x ročně a dále při zjištění slabého místa v zabezpečení osobních údajů, při změně bezpečnostních požadavků, při bezpečnostním incidentu nebo změny v relevantních osobních údajích či hrozeb. V podmínkách společnosti odpovídá MANAŽER KVALITY.
(6) Na základě analýzy hrozeb a zranitelných míst jsou klasifikována následující rizika ochrany osobních údajů, která jsou řazena podle pravděpodobnosti vzniku a intenzity dopadu v podmínkách společnosti GHC.

11.2.3. Riziko neoprávněného nakládání s osobními údaji zaměstnanci určenými pro zpracování osobních údajů

(1) Neoprávněné nakládání s osobními údaji může být buď úmyslné nebo neúmyslné (nedbalostní).
(2) Možné způsoby neoprávněného nakládání s osobními údaji:
- nedodržení bezpečnostních zásad souvisejících s manipulací s osobními údaji v místě jejího výskytu:
- umožnění přístupu nepovolaných osob do prostoru, ve kterém se ukládají a zpracovávají osobní údaje,
- ponechávání neuzamčeného úschovného objektu, ve kterém jsou ukládány dokumenty s osobními údaji,
- neukládání dokumentů s osobními údaji do úschovného objektu,
- umožnění pořizování kopií dokumentů s osobními údaji,
- umožnění nahlížení do dokumentů s osobními údaji,
- neprovádění skartace písemných dokumentů s osobními údaji a stanovené likvidace souborů uložených v počítači,
- zpracovávání osobních údajů pro jiný než stanovený účel,
- zpracovávání osobních údajů nad rozsah nezbytný pro naplnění stanoveného účelu,
- uchovávání osobních údajů nad rámec doby, která je nezbytná k účelu jejich zpracování,
- sdružování osobních údajů, které byly získány k rozdílným účelům,
- nedodržování zásady mlčenlivosti.
- nedodržení bezpečnostních zásad souvisejících s manipulací s osobními údaji mimo prostor jejich zpracování a ukládání (např. přeprava dokumentů z místa zpracování do místa projednání se zákazníkem apod.):
- nedodržení podmínek pro přenášení nebo přepravu dokumentů s osobními údaji,
- umožnění pořizování kopii dokumentů s osobními údaji,
- umožnění nahlížení do dokumentů s osobními údaji,
- ztráta dokumentů s osobními údaji.

(3) Minimalizace těchto rizik se provádí důsledným uplatňováním ustanovení personální bezpečnosti (pečlivým výběrem osob, které budou pracovat s osobními údaji v rámci organizace) a důslednou kontrolní činností v oblasti administrativní bezpečnosti.

11.2.4. Riziko neoprávněného nakládání s osobními údaji nepovolanými osobami

(1) Nepovolanými osobami se rozumí nejen cizí osoby, ale i zaměstnanci společnosti GHC, kteří nejsou určeni ke zpracovávání osobních údajů.
(2) Možné způsoby neoprávněného nakládání s osobními údaji nepovolanými osobami:
- trestná činnost – vloupání do objektu,
- využití nedbalosti zaměstnanců určených pro zpracování osobních údajů ze strany nepovolaných osob,
- průnik do informačního systému,
- přepadení zaměstnance GHC při přenášení nebo přepravě dokumentů s osobními údaji v rámci objektu i mimo objekt GHC,
- přepadení zaměstnance GHC při manipulaci s dokumenty obsahujícími osobní údaje ve vyhrazeném prostoru pro zpracování těchto údajů,
- vydírání zaměstnance GHC nebo nátlak pod výhrůžkou násilí.

(3) Minimalizace těchto rizik se provádí návrhem a důsledným uplatňováním ustanovení technické a informační bezpečnosti, opatřeními zajišťujícími bezpečnost určených zaměstnanců při manipulaci s osobními údaji, režimovými opatřeními a důslednou kontrolní činností.

11.2.5. Riziko neoprávněného nakládání s osobními údaji při vzniku živelní pohromy, provozní nebo průmyslové havárie

(1) Možné způsoby neoprávněného nakládání s osobními údaji při vzniku živelní pohromy nebo havárie:
- poškození osobních údajů,
- znehodnocení osobních údajů,
- zničení osobních údajů,
- poškození úschovného objektu živelní pohromou nebo havárií takovým způsobem, že osobní údaje budou volně přístupné a může dojít k neoprávněné manipulaci s osobními údaji, včetně jejich vyzrazení a zneužití nepovolanou osobou.

(2) Minimalizace těchto rizik je prováděna na základě opatření stanovených havarijními plány objektů a plány kontinuity. Tato opatření jsou zaměřena především na evakuaci osob a dokumentů z postižené oblasti a následné uložení dokumentů na jiná k tomuto účelu určená místa.

11.2.6. Riziko neoprávněného nakládání s osobními údaji při vyhlášení krizového stavu

(1) Možné způsoby neoprávněného nakládání s osobními údaji při vyhlášení krizového stavu dle zákona o krizovém řízení:
- trestná činnost – vloupání do objektu,
- přepadení zaměstnance GHC při přenášení nebo přepravě dokumentů s osobními údaji v rámci objektu nebo mimo objekt GHC,
- přepadení zaměstnance GHC manipulujícího s osobními údaji v určeném prostoru,
- poškození osobních údajů,
- znehodnocení osobních údajů,
- zničení osobních údajů,
- poškození úschovného objektu takovým způsobem, že osobní údaje budou volně přístupné a může dojít k neoprávněné manipulaci s osobními údaji, včetně jejich vyzrazení a zneužití nepovolanou osobou.

(2) Minimalizace těchto rizik je prováděna na základě opatření stanovených havarijními plány objektů a plány kontinuity v návaznosti na opatření stanovená krizovým plánem města Hlavního města Prahy.

(3) Tato opatření jsou zaměřena především na posílení ochrany objektů, přijetí dalších opatření k ochraně určených zaměstnanců GHC a v neposlední řadě i na opatření zaměřená na evakuaci osob a dokumentů a následné uložení dokumentů na jiná k tomuto účelu určená místa.

11.2.7. Riziko vyzrazení osobních údajů pasivním odposlechem nebo nasazením operativní techniky

(1) Možné způsoby neoprávněného nakládání s osobními údaji pasivním odposlechem nebo nasazením operativní techniky:
- nedodržování zásady mlčenlivosti ze strany zaměstnanců GHC,
- přítomnost nepovolané osoby v místnosti při projednávání osobních údajů,

- odposlechnutí projednávání osobních údajů, např. při otevřených dveřích nebo oknech do místnosti,
- instalace odposlechové nebo jiné monitorovací techniky.

(2) Minimalizace těchto rizik se provádí proškolováním určených zaměstnanců GHC, důsledným dodržováním všech režimových opatření, technickými opatření, která znemožňují instalaci odposlechové techniky a následně i její použití.

11.3. Doporučení ke stanovení opatření

(1) MANAŽER KVALITY provede zhodnocení stávajících bezpečnostních perimetrů a se součinností ostatních odpovědných pracovníků stanoví vhodná organizační a technická opatření, určení zdrojů, termínů a odpovědností za splnění opatření.

(2) Při stanovení opatření musí být brána v úvahu úroveň rizika a alespoň tyto varianty zvládání rizik:
- školení, výcvik
- nastavení bezpečnostního perimetru
- omezení související činnosti
- doplnění plánu monitoringu
- přenos rizika na jiný subjekt (např. dodavatel)
- možnost snížení hrozby

(3) Při stanovení opatření musí být vzaty v úvahu také:
- náklady na realizaci opatření musí být efektivní ve vztahu k předpokládané ceně dopadů a významu agend
- požadavky na legislativu a jiné relevantní předpisy
- ohodnocení vnitřních a vnějších závislostí na existujících smlouvách
- provozní omezení
- politika/cíle společnosti

(4) Realizace opatření schvaluje MANAŽER KVALITY**.**

(5) Hodnocení účinnosti opatření se projednává podle stanovených termínů realizace opatření, nejpozději však v intervalu 1x za rok. Odpovídá MANAŽER KVALITY.

XI. TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ

12.1. Povinnosti zaměstnanců a spolupracovníků

(1) Vedoucí úseků, na kterých se provádí zpracování osobních údajů, jsou povinni:

- seznámit podřízené zaměstnance se stanoveným účelem, k němuž jsou osobní údaje zpracovávány, a povinností zpracovávat osobní údaje pouze v souladu s tímto účelem,
- zajistit ochranu osobních údajů před neoprávněným nebo nahodilému přístupu k osobním údajům, jejich změnou, zničením nebo ztrátou, neoprávněným přenosům, případně před jiným zneužitím,
- v rámci své organizační působnosti stanovit prostředky a způsob zpracování osobních údajů a seznámit s nimi své podřízené zaměstnance pověřené zpracováním osobních údajů,
- zabezpečit zpracování osobních údajů pouze se souhlasem subjektu údajů. Bez tohoto souhlasu mohou být osobní údaje zpracovávány pouze v případech uvedených v bodu 5 odst. (6) a (7) této podnikové normy,
- zabezpečit zpracování pouze přesných osobních údajů, ověřovat zpracovávané údaje, a je-li to nezbytné, aktualizovat je. V případě, že při ověřování zjistí, že jím zpracované osobní údaje

nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje.

- při zpracování osobních údajů dbát, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti a na ochranu před neoprávněným zasahováním do soukromého a osobního života,
- zajistit uchovávání osobních údajů pouze po dobu nezbytně nutnou k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné,
- zajistit likvidaci osobních údajů v souladu s Nařízením,
- provádět pravidelné kontroly dodržování Nařízení a této podnikové normy na podřízených pracovištích,

(2) Všichni zaměstnanci a spolupracovníci přebírají odpovědnost za svěřené informační prostředky, které v rámci své pracovní činnosti používají a za bezpečné nakládání s osobními údaji, s nimiž v rámci plnění svých pracovních povinností přicházejí do styku.

(3) Zaměstnanci, kteří v rámci plnění pracovních povinností přicházejí do styku s osobními údaji zpracovávanými v rámci činnosti společnosti, jsou povinni dodržovat ustanovení Nařízení a této podnikové normy.

(4) Zaměstnanci jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost trvá i po skončení zaměstnání nebo příslušných prací.

(5) Při zpracování osobních údajů jsou zaměstnanci povinni dbát, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti a dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

(6) Zaměstnanci jsou povinni zpracovávat osobní údaje pouze za podmínek a v rozsahu stanoveném společností GHC. Zaměstnanci nesmí osobní údaje zpracovávat a využívat pro své soukromé či jiné účely.

(7) Zaměstnanci nesmí umožnit pohyb nepovolaných osob v prostoru, kde jsou osobní údaje zpracovávány nebo ukládány, dále nesmí umožnit nahlížení nepovolaných osob do listin a na monitory počítačů, jestliže nesou osobní údaje jiného subjektu údajů.

(8) Zaměstnancům není dovoleno hlasitě sdělovat osobní údaje ve veřejných prostorách objektů nebo pracovišť společnosti (např. v obchodních kancelářích při jednání se zákazníkem apod.), pokud si to subjekt údajů výslovně nevyžádá.

(9) Zaměstnanci jsou povinni bezprostředně ohlásit svému nadřízenému zaměstnanci každou stížnost, kterou subjekt údajů podá ať ústně nebo písemně v souvislosti s ochranou svých osobních údajů.

(10) Každý zaměstnanec a spolupracovník je dále povinen:

Všeobecně:

- Při manipulaci s písemnostmi dbát na ochranu před ztrátou, odcizením, poškozením nebo znehodnocením.
- Při převozu písemností i přenosných zařízení a médií dbát na bezpečnost a ochranu před odcizením či ztrátou.
- Řídit se ustanoveními uvedenými v této směrnici.

Výpočetní technika

- Práce s výpočetní technikou je popsána v SOP-502 Všeobecná pravidla pro užívání informací.

Přístup do prostor společnosti

- Pokud zaměstnanec vstupuje do objektu společnosti jako první, musí se pro bezpečný přístup identifikovat formou přiložení otisku prstu na čtecí zařízení.
- Pokud zaměstnanec opouští objekt společnosti během nebo po skončení pracovní doby, je povinen zkontrolovat uzavření oken a dveří. V případě, že odchází z objektu jako poslední, je povinen objekt zakódovat na zabezpečovacím zařízení a uzamknout.
- Zaměstnanec má právo vstupovat do uzamčených prostor, které souvisejí s výkonem jeho pracovní činnosti a má dle systému přidělených klíčů a kódů patřičná oprávnění. Pokud vstupuje do uzamčených prostor bez patřičného oprávnění, pak jedině s vědomím a výslovným souhlasem oprávněné osoby.
- nástroje používané k autentizaci (klíče, čipové karty,…) jsou v zásobě pro vydání novým uživatelům.

(11) Zaměstnancům a externím spolupracovníkům je přísně zakázáno:

Všeobecně

- Poskytovat osobní údaje nepovolaným osobám v elektronické, písemné i ústní formě.
- Při převozu písemností nechávat tyto bez dozoru nebo přístupné cizím osobám (např. v odemčeném autě)
- Manipulovat s hardwarovými prostředky a zařízeními (např. router, switch, tiskárna, kabeláž), tj. přesouvat je na jiné místo, odpojovat je ze sítě nebo vstupovat do jejich administrace (pokud je to možné) bez povolení a měnit jejich konfiguraci.

Výpočetní technika

- Práce s výpočetní technikou je popsána v SOP-502 Všeobecná pravidla pro užívání informací.

12.2. Zabezpečení ochrany osobních údajů

Jedná se o opatření směřující jak proti náhodným vlivům, tak proti úmyslnému jednání vlastních zaměstnanců i jakýchkoli jiných osob s cílem zamezit nahodilému nebo neoprávněnému přístupu k osobním údajům, k jejich změně, zničení, ztrátě, neoprávněným přenosům a zpracování, příp. k jinému zneužití osobních údajů.

12.2.1. Personální bezpečnost

(1) Systém opatření, jejichž cílem je stanovit okruh zaměstnanců, kteří se při výkonu své pracovní funkce budou seznamovat s osobními údaji a budou provádět jejich zpracování.

(2) Vedoucí zaměstnanci všech útvarů, na kterých se provádí zpracování osobních údajů, určí pracovní funkce, u kterých je pro plnění pracovních povinností spojených s touto funkcí nezbytné seznamovat se s osobními údaji nebo zpracovávat osobní údaje.

(3) Se zaměstnanci, u nichž je výkon jejich funkce spojen s přístupem k osobním a citlivým údajům, je uzavřena pracovní smlouva, případně její dodatek, s ustanovením o ochraně osobních údajů.

12.2.2. Administrativní bezpečnost

(1) Systém opatření, jejichž cílem je ochrana osobních údajů při jejich zpracovávání.

(2) Osobní údaje se v GHC vyskytují jak v listinné, tak i elektronické podobě.

(3) Účelem je stanovit podmínky, rozsah a kompetence jednotlivých zaměstnanců, kteří přicházejí při své práci do styku s osobními údaji.

(4) Podmínky pro manipulaci s osobními údaji a jejich ukládání:

a) osobní údaje mohou zpracovávat pouze osoby, které tím pověří GHC a které mají uzavřenu smlouvu v souladu s Nařízením,

b) zpracování osobních údajů se provádí bez přítomnosti nepovolaných osob; zaměstnanec je povinen zamezit přístupu nepovolaných osob k osobním údajům,

c) provádí se pouze operace související se stanoveným zpracováním osobních údajů,

- při zpracování osobních údajů prostřednictvím výpočetní techniky se využívají možnosti aplikací k ochraně souborů s osobními údaji, spořič obrazovky chráněný heslem atd.
- po ukončení práce se písemnosti nebo nosiče obsahující osobní údaje uzamykají do úschovných objektů (odděleně od ostatních písemností). Klíče od úschovných objektů mají pouze pověření zaměstnanci GHC
- při ztrátě klíčů nebo jejich duplikátů je nutné.
  - neprodleně oznámit tuto skutečnost nadřízenému zaměstnanci,
  - umístit všechny písemnosti a nosiče obsahující osobní údaje do jiného úschovného objektu (do doby nalezení klíčů nebo rozhodnutí nadřízeného zaměstnance),
  - není-li to z technických nebo jiných důvodů možné, musí být ochrana písemností nebo nosičů obsahujících osobní údaje zajištěna jiným způsobem, např. musí být dosavadní uzávěry nebo zámky vyměněny.

(5) V situaci, že se osobní údaje (např. dokumenty klientů, zaměstnanců) přepravují osobními vozy, je řidič vozidla povinen:

- v případě opuštění vozu uzamknout vozidlo, když se vzdálí od vozidla
- při opuštění vozu zapnout funkci bezpečnostního alarmu (pokud je vozidlo vybaveno)
- je výslovně zakázáno ponechávat osobní údaje bez dozoru ve voze.

(6) V situaci, že se osobní údaje (např. dokumenty klientů, zaměstnanců) přepravují veřejnou přepravou nebo pěšky, je osoba povinna:

- nevzdalovat se od osobních údajů, mít je stále při sobě na blízku
- nepůjčovat nebo nepověřovat cizí osoby k ohlídání nebo přenášení aktiv

(7) Při ukončení pracovního poměru zaměstnance pověřeného zpracováním osobních údajů nebo při převodu na jiné pracovní místo se provede předání všech písemností obsahujících osobní údaje.

(8) Příslušné kompetence a odpovědnost zaměstnanců GHC při zpracování osobních údajů určuje v souladu s jejich pracovním zařazením Organigram (příloha č.2 SOP-518 Příručka kvality laboratoře), dále pak pracovní smlouvy a Náplně práce (formulář F-03B Popis pracovní funkce)

(9) Další doporučená opatření k zajištění administrativní bezpečnosti jsou uvedena v příloze č. 1 a 2.

12.2.3. Technická bezpečnost

(1) Systém opatření, jejichž cílem je zabezpečení ochrany osobních údajů technickými prostředky.

(2) Technická opatření vychází z požadavku rozumné míry ochrany osobních údajů.

(3) Zabezpečení objektu a kanceláře tak, aby nemohlo dojít k neoprávněnému nebo nahodilému vstupu nepovolaných osob a k možnému zneužití zde uložených osobních údajů.

a) Klasickou ochranu představují mechanické zábranné prostředky:
- bezpečnostní uzamykací systémy,
- bezpečnostní systémy dveří,
- mříže,
- bezpečnostní folie,
- trezory, bezpečnostní schránky a další úschovné objekty.

b) Technickou ochranu představují:

- elektrická zabezpečovací signalizace,
- elektrická požární signalizace,
- elektronická kontrola vstupu,
- kamerový systém.

(4) Zabezpečení ochrany se posuzuje vždy souhrnně. Absence některého z výše uvedených prostředků neznamená nedostatečnou ochranu osobních údajů.

(5) Technické zabezpečení ochrany osobních údajů na jednotlivých pracovištích v rámci společnosti schvaluje MANAŽER KVALITY.

(6) Další doporučená opatření k zajištění technické bezpečnosti jsou uvedena v příloze č. 1 a 2.

12.2.4. Informační bezpečnost

(1) Zabezpečení ochrany osobních údajů při zpracování osobních údajů pomocí výpočetní techniky na jednotlivých pracovištích v rámci společnosti dokumentuje a schvaluje Technik IT.

(2) Základní opatření informační bezpečnosti:

- Přístup k osobním údajům je chráněn systémem přístupových účtů, hesel a práv stanovených v rozsahu potřebném pro plnění úkolů jednotlivých zaměstnanců GHC.
- Přístupová práva přidělují pouze pověření zaměstnanci společnosti.
- Antivirová ochrana je prováděna na uživatelských stanicích i na serverech, během provozu je prováděna rezidentní kontrola přijímaných a odesílaných dat.
- Je prováděna ochrana dat před průnikem z Internetu.
- Provádí se pravidelné zálohování dat viz 02-17 Plán zálohování.
- Není doporučeno zálohovat dokumenty obsahující osobní údaje přes cloudové služby. Fyzické umístění serverů je obtížně dohledatelné a Správce osobních údajů ručí za bezpečnost i takto uložených dat.
- Záložní kopie dat musí být zabezpečena proti neoprávněnému přístupu a čtení.

(2) Za zajištění antivirové ochrany lokálních stanic na centrále společnosti nese odpovědnost Technik IT a u serverových aplikací Technik IT. U externích kanceláří nese odpovědnost uživatel.

(3) Technik IT definuje použité systémy ochrany, jejich rozsah a úroveň (parametry nastavení), dále určuje pravidla pro jejich používání a aktualizaci.

(4) Za dodržování všeobecných zásad antivirové ochrany při zpracování a používání elektronických informací je odpovědný každý uživatel.

(5) Povinnosti uživatelů jsou definovány v kap. 12.1.

(6) Ochrana před zneužitím osobních údajů externími subjekty – v případě, že při instalaci či údržbě systému nebo příslušné aplikace přijdou externí subjekty do styku s osobními údaji, je třeba uzavřít s těmito externími subjekty smlouvu týkající se ochrany a utajení informací, včetně příslušné finanční sankce za nedodržení této povinnosti a možnost náhrady vzniklé škody.

(7) Další doporučená opatření k zajištění bezpečnosti IT jsou uvedena v příloze č. 1 a 2.

XII. PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ

13.1. Předávání osobních údajů do jiných států

(1) Volný pohyb osobních údajů nemůže být omezován, pokud jsou údaje předány do členského státu Evropské unie.

(2) Předávání osobních údajů do určité třetí země nebo určité mezinárodní organizaci se může uskutečnit, jestliže tato třetí země, určité území nebo jedno či více konkrétních odvětví v této třetí zemi, nebo tato mezinárodní organizace zajišťují odpovídající úroveň ochrany. Takovéto předání nevyžaduje žádné zvláštní povolení.

(3) Správci, kteří jsou součástí skupiny podniků nebo instituce přidružené k ústřednímu orgánu, mohou mít oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců.

(4) Předávání osobních údajů do třetích zemí nebo organizací je možné pouze za dodržení podmínek stanovených Nařízením a na základě dohod, které zahrnují vhodné záruky pro subjekty údajů a za podmínky, že jsou práva subjektu údajů vymahatelná a je účinná i právní ochrana subjektu údajů.

13.2. Předávání osobních údajů Policii České republiky

(1) V souladu s ustanovením zákona o ochraně osobních údajů se v tomto případě jedná o zpracování osobních údajů bez souhlasu subjektu údajů.

(2) GHC jako správce osobních údajů je povinna dodržet zákonem stanovený požadavek, jehož obsahem je prokázat komu, kdy a za jakým účelem předala zpracovávané osobní údaje.

(3) Stanovený postup pro předávání osobních údajů Policii České republiky:

- žádosti o předávání osobních údajů Policii v žádném případě nesmí být vyřizovány na základě neověřeného telefonického dotazu,
- osobní údaje by měly být Policii předávány vždy pouze písemnou formou a uchovávány v GHC, včetně odpovědi příslušného správce nebo zpracovatele. Z uvedené dokumentace musí být jasně patrno:
    - komu byly osobní údaje předány (*identifikační údaje o útvaru Policie nebo policistovi, který o výdej údajů zažádal*),
    - kdy (*kdy byla žádost o předání osobních údajů přijata*),
    - za jakým účelem byl výdej osobních údajů žádán (*musí odpovídat potřebám plnění jejího konkrétního úkolu*),
    - rozsah požadovaných osobních údajů ze strany Policie *(jaké osobní údaje byly na žádost Policie předány)*,
    - kdy, kým a jakým způsobem byla žádost o výdej osobních údajů vyřízena.
- v případě osobního jednání s policistou je třeba, aby GHC obdržela kopii úředního protokolu.

XIII. PROBLEMATIKA VZTAHUJÍCÍ SE K OCHRANĚ OSOBNÍCH ÚDAJŮ

14.1. Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech

(1) Novelou zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech byla stanovena pravidla pro nakládání s rodnými čísly a využívání rodných čísel.

(2) Rodné číslo je oprávněna užívat nebo rozhodovat o jeho využívání výlučně fyzická osoba, které bylo rodné číslo přiděleno nebo její zákonný zástupce.

(3) Rodné číslo lze v souladu s novelou zákona využívat pouze v těchto případech:

- jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřebu vedení Centrální evidence závětí,

- stanoví-li tak zvláštní zákon,
- v souladu s tímto ustanovením mohou rodná čísla využívat i jiné orgán a instituce. Jde např. o Policii ČR, Státní zastupitelství, zdravotní pojišťovny, zdravotnická zařízení, banky, pojišťovny, telekomunikační operátoři, veřejnoprávní korporace jako jsou různé profesní komory. Pokud tento zvláštní zákon stanoví možnost volit mezi údaji (např. rodné číslo nebo datum narození) je pouze na vůli nositele rodného čísla, který z uvedených údajů poskytne.
- se souhlasem nositele rodného čísla nebo jeho zákonného zástupce.
- Souhlas musí být svobodným a vědomým projevem vůle nositele rodného čísla s využíváním rodného čísla.

14.2. Zpracování osobních údajů za účelem nabízení obchodu nebo služeb

(1) Provádí-li GHC zpracování osobních údajů za účelem nabízení obchodu nebo služeb, lze pro tento účel použít osobní údaje na základě souhlasu subjektu údajů. Osobní údaje je možné za účelem přímého marketingu zpracovávat bez souhlasu jen v případě, jedná-li se o oprávněný zájem Správce či zpracování během jednání o uzavření smlouvy.

(2) V podmínkách společnosti GHC dochází nebo může docházet k následujícím typům zpracování osobních údajů za účely přímého marketingu (především zasílání newsletterů či přímému kontaktování):

- Oslovování stávajících klientů s nabídkami a informacemi, které souvisí s produktem či službou, kterou klient v minulosti zakoupil. Takové zpracování je v rámci oprávněného zájmu Správce.
- Oslovování subjektů, kteří se dobrovolně přihlásili k odběru. Přihlášením k odběru novinek subjekt údajů vyslovil svobodnou vůli s tímto zpracováním. U formuláře na přihlášení o odběru novinek je odkaz na informace o zpracování OÚ (viz formulář GDPR_F-05).
- Oslovování subjektů, se kterými začalo jednání o možné budoucí spolupráci – tzn. jednání o uzavření smlouvy. Takovéto kontakty mohou být získány během obchodní činnosti např. během účasti na veletrhu aj. V případě neuzavření smlouvy je třeba vyhodnotit, zda existuje oprávněný zájem na dalším uchovávání osobních údajů potenciálního klienta (např. eventuální budoucí obnovení jednání o smlouvě). Po určitou dobu po ukončení jednání o smlouvě je možné zpracovávat, resp. dále uchovávat tato data z titulu oprávněného zájmu na zpracování osobních údajů pro účely budoucího obchodního využití, toto uchování by však nemělo být neomezené a rámcově by nemělo přesáhnout dobu několika málo let.
- Oslovování subjektů, kteří neprojevili z vlastní iniciativy zájem o uzavření smlouvy. Během tohoto zpracování (zařazení do databáze společnosti) je třeba velice pečlivě zvážit, zda oprávněný zájem správce (GHC) nepřevyšuje zájmy a svobody dotčené osoby. V případě neuzavření smlouvy se dále postupuje jako v předchozím bodu.
- Oslovování subjektů, kteří neprojevili z vlastní iniciativy zájem o uzavření smlouvy a zároveň není zřejmé, že dojde ke střetu zájmu správce a dotčeného subjektu údajů. S takovýmto zpracováním je nutné získat souhlas.

(3) Veškeré odesílané newslettery obsahují v zápatí možnost se z odběru odhlásit. Zároveň je uveden odkaz na informace o zpracování OÚ (viz formulář GDPR_F-05).

(4) Společnost, která zpracovává tyto osobní údaje, může tyto údaje předat jinému správci pouze na výslovnou žádost subjektu údajů nebo pokud mu to zákon ukládá (např. poskytnutí informací orgánům činným v trestním řízení). Jiný správce, kterému byly předány údaje dle tohoto odstavce, nesmí tyto údaje předávat jiné osobě.

(5) Propojování databází zpracovatelem při zpracovávání osobních údajů pro různé správce je dle Nařízení nepřípustné.

(6) V souladu s odstavcem (48) GDPR mohou mít Správci, kteří jsou součástí skupiny podniků nebo instituce přidružené k ústřednímu orgánu, oprávněný zájem na předání osobních údajů v rámci skupiny podniků pro vnitřní administrativní účely, včetně zpracování osobních údajů zákazníků či zaměstnanců.

14.3. Kopírování občanských průkazů a cestovních dokladů

(1) Uchovávání kopie osobního dokladu je považováno za zpracování osobních údajů dle Nařízení, které by mělo stejně jako jiné druhy zpracování probíhat pouze v jeho intencích a v souladu s platným zvláštním právním předpisem.

(2) Dle ustanovení zákona o občanských průkazech a zákona o cestovních dokladech je zakázáno pořizovat jakýmikoliv prostředky kopie občanského průkazu nebo cestovního dokladu bez souhlasu občana, kterému byl občanský průkaz nebo cestovní doklad vydán, pokud zvláštní právní předpis nebo mezinárodní smlouva, kterou je Česká republika vázána, nestanoví jinak. Toto ustanovení u obsahu pojmu souhlas odkazuje na definici souhlasu dle Nařízení.

(3) Zvláštním právním předpisem dle předchozího odstavce je např. zákon č. 253/2008 Sb. o některých o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, který upravuje podmínky pro provádění identifikace fyzických osob a uchovávání stanovených údajů prostřednictvím kopií dokladů, a dále např. notářský řád, zákon č. 21/2006 Sb., o ověřování shody opisu nebo kopie s listinou a o ověřování pravosti podpisu a o změně některých zákonů (zákon o ověřování).

(4) Rozhodne-li se GHC uchovávat kopie výše uvedených dokladů stává se dle zákona o ochraně osobních údajů správcem a musí dodržovat veškeré povinnosti související s nařízením.

14.4. Evidence při vstupech do budov

(1) Vstupy zaměstnanců jsou evidovány v docházkovém systému díky autentizaci pomocí otisku prstu. Evidence návštěv či jiných subjektů není evidována, za návštěvu odpovídá dotčený zaměstnanec.

14.5. Zpracování osobních údajů zaměstnanců

(1) Životopisy zasílané uchazeči o pracovní pozici nabízenou zaměstnavatelem, je nutné po ukončení výběrového řízení řádně skartovat nebo v případě uchování definovat platný účel a zajistit souhlas s tímto uchováním (GDPR_F-08).

(2) Uzavřením pracovní smlouvy, dohody o provedení práce, dohody o pracovní činnosti vzniká pracovněprávní vztah mezi zaměstnavatelem a zaměstnancem. V důsledku toho dochází ke zpracování osobních údajů zaměstnanců zaměstnavatelem. Jedná se například o zpracování osobních údajů v rámci osobního spisu zaměstnance, který obsahuje pracovní smlouvu, platové výměry, doklady o vzdělání apod.

(3) Tyto osobní údaje slouží pro zpracování výstupů v oblasti mzdové, daňové, důchodového, nemocenského a zdravotního pojištění na základě zvláštních zákonů (např. zákon č. 262/2006 Sb., zákoník práce, zákon č. 586/1992 Sb., o daních z příjmů, zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, zákon č. 155/1995 Sb., o důchodovém pojištění apod.).

(4) Potvrzení lékaře nebo zdravotnického zařízení ze vstupní nebo preventivní lékařské prohlídky o tom, že zaměstnanec je schopen vykonávat svou práci, není zvláštním údajem vypovídajícím o zdravotním stavu zaměstnance.

(5) Výpis z rejstříku trestů, který dokládá beztrestnost, není zvláštní osobní údaj dle Nařízení. V případě, že zaměstnavatel vyžaduje od svých zaměstnanců předložení výpisu z rejstříku trestů pro ověření způsobilosti pro výkon určitého zaměstnání v souladu s příslušným ustanovením zákoníku práce, zákona č. 262/2006 Sb., není nutný souhlas.

(6) Citlivý osobní údaj „národnost“ není potřebný k žádnému zákonnému účelu zpracování za účelem personální práce zaměstnavatele. V rámci zaměstnávání cizích státních příslušníků dochází ke zpracování údaje „státní příslušnost“, tento údaj je vyžadován v souladu se zvláštním zákonem (např. zákon č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, zákon č. 435/2004 Sb., o zaměstnanosti apod.) není nutný souhlas.

(7) Pokud jsou osobní údaje zaměstnance zpracovávány za účelem firemní prezentace, je nutné zajistit souhlas zaměstnanců s tímto zpracováním. Může jít o kontakty či fotografie na webu, sociálních sítích, propagačních materiálech aj.

(8) Pokud jsou v prezenčních listinách nebo osvědčeních vydávaných zaměstnavatelem nebo jeho dodavatelem školicích služeb potřeba uvádět osobní údaje pro přesnou identifikaci školené osoby, uvádí se „jméno“, „příjmení“, „osobní číslo“ a případný „podpis“.

14.6. Pořízení a užití fotografií zaměstnanců či jiných subjektů

(1) V rámci společnosti GHC (např. zveřejnění fotografií na webových stránkách, sociálních sítích či tištěných propagačních materiálech) je možný pouze tento postup:

- získat souhlas subjektu údajů se zveřejněním (pro účely propagace) nebo
- fotografii užít v souladu § 89 Zákona č. 89/2012 Sb. (např. za účelem vydání informačního či zpravodajského článku)

14.7. Jubilea a společenské rubriky

(1) Dle ustanovení Nařízení je GHC povinna zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje pouze v mezích 5 odst. (6) nebo pokud k tomu dal subjekt údajů předem souhlas.

(2) V rámci GHC (např. při užití data narození či křestního jména k blahopřání) je možný postup získat souhlas subjektu údajů s užitím OÚ za těmito účely.

14.8. Zpracování osobních údajů zemřelých osob

(1) Nařízení nestanoví přechod práv subjektu údajů po jeho úmrtí na jiné osoby, tzn. že po úmrtí subjektu údajů pozbývají platnosti ta ustanovení Nařízení, v nichž subjekt údajů vystupuje jako účastník občanskoprávních vztahů (jedná se o ustanovení o právech subjektu údajů a povinnostech správce ve vztahu k subjektu údajů, konkrétně se jedná o souhlas se zpracováním osobních údajů, souhlas se zpracováním citlivých údajů, informační povinnost správce, ochrana práv subjektu údajů a náprava nemajetkové újmy).

(2) Při zpracování osobních údajů zemřelých osob zůstávají v platnosti ta ustanovení Nařízení, ve kterých subjekt údajů nevystupuje jako účastník občanskoprávních vztahů (jedná se především o některé povinnosti správce, povinnosti při zabezpečení osobních údajů).

(3) V GHC může nastat během zpracování osobních údajů následující situace:

- dojde-li k úmrtí subjektu údajů a nedostane-li GHC tuto informaci ihned, zjistí ji po určitém časovém období, protože je podle Nařízení povinna ověřovat, zda jsou údaje přesně s ohledem na stanovený účel,
- společnost je dle Nařízení povinna uchovávat údaje pouze po dobu, která je nezbytně nutná k účelu jejich zpracování. Tento účel mohl, ale nemusel smrtí subjektu údajů pominout:

- pokud účel zpracování údajů nepominul, provádí GHC dále zpracování osobních údajů dle Nařízení (*jde např. o uplatnění zákonných práv nebo plnění zákonných povinností samotného správce, jako je třeba uchování účetních dokladů apod*.)
- pokud účel zpracování údajů pominul, je GHC povinna provést likvidaci osobních údajů.

14.9. Kamerové systémy

14.9.1. Základní ustanovení

(1) Kamerové sledování fyzických osob je zpracováním osobních údajů podle Nařízení. S tím zároveň souvisí aplikace jiných právních předpisů, zejména občanského zákoníku upravujícího podmínky ochrany osobnosti nebo povinnost označit prostory monitorované kamerovým systémem informační tabulkou, např. „Prostor je monitorován kamerovým systémem“. Provozovatelem kamerového systému je GHC.

(2) Provozování kamerového systému je považováno za zpracování osobních údajů, i když je vedle monitorování prováděn i záznam pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

(3) Údaje uchovávané v záznamovém řízení jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo nebo nepřímo identifikovat konkrétní fyzickou osobu. Fyzická osoba je identifikovatelná, pokud ze snímku nebo jiného obrazového záznamu, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej fyzické osoby) a na základě propojení s dalšími disponibilními údaji je možná plná identifikace osoby.

(4) Zpracování osobních údajů provozováním kamerového systému je přípustné:

- v rámci plnění úkolů uložených zákonem, např. zákonem č. 273/2008 Sb., o Policii ČR, zákonem č. 553/1991 Sb., o obecní policii, zákonem č. 412/2005 Sb., o ochraně utajovaných informací, zákonem č. 224/2015 Sb., o prevenci závažných havárií apod.,
- na základě řádného souhlasu subjektu údajů,
- pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.

14.9.2. Povinnosti správce při provozování kamerového systému se záznamovým zařízením

(1) Stanovit účel:

- Účel pořizování záznamů musí korespondovat s důležitými právem chráněnými zájmy správce *(např. ochrana majetku před krádeží)*.
- Záznamy mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité právem chráněné zájmy správce.
- Data získaná z kamerových systémů nesmějí být využívána za jiným účelem, než je stanovený účel *(např. záznamy získané za účelem ochrany majetku nemohou být využívány k marketingovým účelům apod.)*.
- Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem (např. boj proti pouliční kriminalitě apod.). Předávání záznamů z kamerových systémů třetím osobám je možné pouze v případech povolených zákonem (např. předávání údajů Policii ČR, předávání údajů na základě soudního příkazu apod.).

- Kamerové systémy lze použít k ochraně majetku za splnění těchto podmínek:
    - nesmí dojít k zásahu do ochrany soukromí zaměstnance, případně jiné fyzické osoby.
    - *kamery není možné instalovat tam, kde má zaměstnanec, případně jiná fyzická osoba, právo na soukromí, např. v šatnách, sprchách, toaletách, kuchyňkách a v podobných prostorech.*
    - účelu, který se získá instalací kamerového systému, nelze dosáhnout jinak.
    - kamerový systém musí být přiměřeným prostředkem k zajištění bezpečnosti předmětu ochrany. Může být využíván pouze tehdy, nejsou-li realizovatelné, dostatečně účinné nebo postačující ostatní bezpečnostní prostředky *(např. majetek je možno chránit před odcizením uzamčením místnosti apod.)*. Instalované kamery musí být umístěny tak, aby zorná pole jejich objektivu zobrazovala pouze záběry nezbytně nutné pro stanovený účel.

(2) Stanovit lhůtu pro uchování záznamů:

- Doba uchování záznamů by neměla přesáhnout časový limit přípustný pro naplnění účelu provozování kamerového systému.
- Data by měla být uchovávána v rámci časové smyčky (např. 24 hodin), pokud jde o trvale střežený objekt, nebo případně i dobu delší, v zásadě ne však přesahující několik, nejde-li o pořizování záznamů podle zvláštního zákona, a po uplynutí této doby vymazána.
- Pouze v případě vzniku bezpečnostního incidentu mohou být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu.

(3) Stanovit a zdokumentovat ochranu záznamů:

- Zajistit ochranu snímacího zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním.
- Kamerový systém musí mít stanovenu konkrétní osobu odpovědnou za kamerový systém. Osoba odpovědná za kamerový systém je povinna učinit nebo zajistit veškerá nezbytná technická a organizační opatření k zajištění ustanovení tohoto bodu.
- K monitorům zobrazujícím kamerové záznamy mohou mít přístup pouze k tomu určené osoby (osoba odpovědná za kamerový systém, zaměstnanci ostrahy apod.).
- Ochrana nosičů záznamů:
    - Datové nosiče musejí být uloženy a uchovávány na bezpečném a uzamčeném místě. Klíč od těchto prostor má k dispozici pouze osoba odpovědná za kamerový systém.
    - Při ukládání záznamů z kamer v počítačích je třeba dodržet tyto zásady:
        - vyhradit pro tyto záznamy místo na příslušném serveru,
        - přístup k těmto záznamům má nastavena pouze osoba odpovědná za kamerový systém, a přístup je chráněn systémem přístupových účtů a hesel,
        - musí být provedena ochrana těchto záznamů před průnikem z Internetu,
        - musí být zajištěna ochrana přenosových cest,
        - za provedení dostatečných ochranných opatření přenosových cest a míst uložení na příslušném serveru odpovídá Technik IT
    - Videozáznamy z kamer musí být vymazány vždy do 30 dnů od pořízení záznamu. Tato lhůta je postačující ke zjištění škody na majetku společnosti, případně na zdraví nebo životě zaměstnance nebo ostatních fyzických osob.

- Provádět pravidelné kontroly dodržování přijatých opatření k ochraně záznamů a dále provádět kontrolu příslušných kamer, zda nedošlo k neoprávněné manipulaci s kamerou, např. zda kamera po zásahu neoprávněné osoby (ať již úmyslně nebo neúmyslně) nesnímá jiný prostor, než pro který byla instalována.

(4) Informační tabulka: Informace o monitorování objektu musí být uvedeny na přehledných místech, tj. u všech vstupů/vjezdů a následně pro přehlednost na nástěnce. Pro názornost je možné doplnit písemné informace jednoduchými a názornými obrázky. Stejně tak může správce informovat subjekty elektronickou formou. Je potřeba uvést kontakt na provozovatele systému, účely zpracování, kategorie dotčených osobních údajů a jejich příjemce. Pokud to bude nezbytné pro transparentnost zpracování údajů, měla by být uvedena doba uložení osobních údajů, oprávněné zájmy správce nebo třetí strany.

(5) Garantovat další práva subjektu údajů, zejména právo subjektu údajů na přístup k zpracovávaným datům a právo na námitku proti jejich zpracování.

(6) Kamerové systémy a další monitorovací zařízení podléhá pravidelné údržbě a kontrole funkčnosti ze strany správce osobních údajů.

14.10. Monitorování pohybu služebních automobilů pomocí GPS

(1) Ve společnosti není relevantní.

14.11. Archivace a skartace

(1) Archivace a ukládání písemných dokumentů musí být zabezpečeno v souladu s předpisy a nastavit vhodná technická a organizační opatření. Mezi vhodná technická opatření je možné zařadit fyzické zabezpečení (zámky, závory, mříže, bezpečnostní folie aj.) nebo monitoring prostor (kamerové systémy, pohybová čidla, kouřová čidla, teplotní čidla aj.). V rámci organizačních opatření je nutné omezit přístup zaměstnanců do těchto prostor a oprávněným pracovníkům smluvně definovat odpovědnosti a povinnosti spojené se správou archivu. Správu archivu má ve společnosti GHC na starosti MANAŽER KVALITY.

(2) Je nutné dokumenty označovat a skartovat dle platného Typového skartačního rejstříku, aby nedocházelo k bezdůvodnému ukládání osobních údajů bez specifikovaného účelu zpracování.

(3) Po uplynutí skartační doby je nutné dokumenty předat ke skartačnímu řízení. O provedené skartaci musí být proveden záznam.

(4) Pravidla pro skartaci platí i pro elektronickou verzi dokumentů. Při výmazu starých dokumentů z elektronického archivu se musí vzít v úvahu i všechny zálohy elektronických dat.

(5) Pro elektronickou archivaci platí:

- je oddělena archivace a zálohování dat
- archivní data jsou popsána
- je možné provádět archivaci na různá místa
- archivní data jsou zabezpečena proti neoprávněnému přístupu a čtení
- archivní data jsou chráněna pro případ mimořádných událostí
- je prováděno testování čitelnosti archivovaných dat

(6) Pravidla pro skartaci blíže popisuje SOP-500 Metodika řízení dokumentace.

14.12. Monitorování chodu a používání informačních systémů

(1) V souladu s článkem 13 Listiny základních práv a svobod „Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných

poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

(2) Výpočetní technika je vlastnictvím GHC a zaměstnanci nemají právo tohoto zařízení využívat k jiným účelům než k těm, které vyplývají z jejich pracovního zařazení. V souladu s ustanoveními zákoníku práce jsou zaměstnanci povinni plně využívat pracovní doby a výrobních prostředků k vykonávání svěřených prací.

(3) GHC má právo sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Pro výkon tohoto práva nemá GHC právo sledovat, monitorovat a zpracovávat obsah korespondence zaměstnanců, může ale sledovat počet e-mailů došlých a odeslaných u svých zaměstnanců včetně adresátů odeslané a odesílatelů došlé elektronické pošty.

(4) GHC má právo za účelem správného, efektivního a bezpečného provozování informačních systémů sledovat chod jeho jednotlivých komponent, jejich využívání a odchylky v chování.

14.13. Řízení bezpečnostních incidentů

(1) *Bezpečnostní incident* = jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost ohrožení osobních údajů.

(2) Zjištěné bezpečnostní incidenty a nedostatky musí být nahlášeny MANAŽEROVI KVALITY, zarchivovány, zdokumentovány, prozkoumány a odstraněny s ohledem na příčiny, které je vyvolaly tak, aby mohlo být dosaženo nápravy.

(3) Rozlišení bezpečnostních incidentů (včetně příkladů):
- **Podle cíle:** aktivní (přerušení dostupnosti, narušení integrity, modifikace), pasivní (odposlech)
- **Podle charakteru:** úmyslné, způsobené, nevědomostí, nedbalostí, neznalostí
- **Podle způsobených škod:** vir, červ, trojský kůň, spam, DOS (Denial of service attacks), sniffing, password cracking, zkompromitování uživatelského účtu, phishing a pharming, porušení autorských práv, porušení občanských práv, zákonů apod.

(4) Evidenci záznamů o výskytu a způsobu řešení závažných nebo často opakujících se bezpečnostních incidentů vede MANAŽER KVALITY.

(5) Povinnost oznámení a upozornění na bezpečnostní incidenty má každý zaměstnanec a externí spolupracovník. Správce OÚ dále plní ohlašovací povinnosti dle kapitoly 9.4.

XIV. Monitoring

15.1. Průběžný monitoring

(1) Činnosti monitoringu jsou definovány v SOP-512 Zabezpečení informačních prostředků a souvisejícím plánu monitoringu (11-15 Monitoring)

15.2. Přezkoumávání systému zabezpečení osobních údajů

(1) Vedení společnosti GHC zajišťuje v pravidelných intervalech, nejméně však 1x rok přezkoumávání systému zabezpečení osobních údajů prostřednictvím externí spolupráce.

(2) V rámci přezkoumávání musí být prověřena všechna pracoviště a agendy osobních údajů, které se na pracovištích zpracovávají.

(3) Prověřovatel v dostatečném předstihu zpracuje plán prověrek a předloží k odsouhlasení VEDENÍ SPOLEČNOSTI, poté předá informace o plánovaných prověrkách odpovědným pracovníkům za zpracovávané osobní údaje, případně upraví plán podle časových možností prověřovaných osob.

(4) Odpovědní pracovníci jsou povinni plně spolupracovat s pověřovatelem a poskytovat jim k tomu potřebné kompletní a pravdivé informace.

(5) Výsledky prověrek jsou zdokumentovány v závěrečné zprávě (protokolu) vypracované prověřovatelem. Protokol je předán MANAŽEROVI KVALITY, který ji projedná s vedením společnosti.

(6) Vedení společnosti následně rozhodne o nápravě a případných nápravných opatřeních v případě nalezených nedostatků v systému ochrany osobních údajů.

XV. Související dokumentace

Analýza osobních údajů a analýza rizik
Doplněk / dodatek smluv
Seznam zpracovatelů a třetích osob
Upozornění do emailu
Registr externích předpisů
Plán implementace

XVI. Související formuláře

F-500 Hlášení porušení zabezpečení osobních údajů dozorovému úřadu
F-501 Hlášení porušení zabezpečení osobních údajů subjektu údajů
F-502 Záznam o činnostech zapracování OÚ
F-503 Informace o zpracování OÚ_zaměstnanci
F-504 Informace o zpracování OÚ_obchodní partneři
F-505 Souhlas ke zpracování OÚ_zaměstnanci
F-506 Souhlas ke zpracování OÚ_klienti
F-507 Souhlas ke zpracování OÚ_uchazeči
F-508 Jmenování Pověřence pro ochranu osobních údajů (DPO)

XVII.Přílohy

Příloha č. 1 – Další doporučená technická a IT zabezpečení
Příloha č. 2 – Pravidla nakládání s osobními údaji