Zásady ochrany fyzických osob při zpracování osobních údajů
v Jednotě, spotřebním družstvu v Mikulově (dále jen „Družstvo“)

I. Úvodní ustanovení

1. Tyto Zásady ochrany fyzických osob při zpracování osobních údajů (dále jen „**Zásady**“) jsou informativním textem pro účely zveřejnění na webových stránkách Družstva, který upravuje podmínky ochrany osobních údajů a nakládání s nimi.
2. Tyto Zásady stanoví základní podmínky (povinnosti) a odpovědnost konkrétních zaměstnanců či jiných osob při zpracování osobních údajů v Družstvu, a to v souladu s nařízením Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, dále jen „**GDPR**“), zákonem č. 110/2019 Sb., o zpracování osobních údajů (dále jen „**zákon o zpracování OÚ**“), jakož i se souvisejícími předpisy.
3. Podrobnější pravidla ochrany osobních údajů stanoví zvláštní vnitřní předpisy Družstva.
4. Vzhledem k tomu, že Družstvo zpracovává osobní údaje, je Družstvo při jejich zpracování správcem osobních údajů.

II. Základní pojmy

1. Pro účely těchto Zásad se rozumí:
   a. **„osobními údaji“** veškeré informace o identifikované nebo identifikovatelné fyzické osobě; 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 jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;
   b. **„zvláštní kategorií osobních údajů“** osobní údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení nebo členství v odborech, jakož i genetické údaje, biometrické údaje, údaje o zdravotním stavu či sexuálním životě nebo sexuální orientaci fyzické osoby;
   c. **„subjektem údajů“** fyzická soba, k níž se osobní údaje vztahují (může se jednat o zaměstnance, zákazníka, člena družstva apod.);
   d. **„zpracováním“** jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů; jedná se např. o 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 (toto však není vyčerpávající seznam);

e. **„dalším zpracováním“** zpracování osobních údajů za jiným účelem, než pro který byly původně shromážděny, např. další zpracování volně dostupných údajů (veřejných údajů z katastru nemovitostí, které byly původně shromážděny za účelem vedení evidence katastru nemovitostí apod.);

f. **„správcem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám, nebo společně s jinými určuje účely a prostředky zpracování osobních údajů;

g. **„zpracovatelem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce; za určitých podmínek může být Družstvo i v pozici zpracovatele nebo se může jednat např. o subjekt, který pro Družstvo zajišťuje účetnictví apod.;

h. **„příjemcem“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli; např. OSSZ, FÚ, daňové či celní orgány apod.;

i. **„dozorovým úřadem“** nezávislý orgán veřejné moci zřízený členským státem podle článku 51 GDPR, v případě České republiky Úřad pro ochranu osobních údajů;

j. **„profilováním“** jakákoliv 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; profilováním je např. automatické monitorování chování návštěvníků webových stránek za účelem sledování jejich preferencí a následného zasílání obchodních nabídek;

k. **„pseudonymizací“** 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;

l. **„třetí stranou“** fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jenž je oprávněna ke zpracování osobních údajů;

m. **„porušením zabezpečení osobních údajů“** porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů;

n. **„zaměstnancem“** zaměstnanec Družstva vykonávající práci v pracovním poměru, případně osoby konající práci pro Družstvo na základě dohod o pracích konaných mimo pracovní poměr.

III. Základní zásady ochrany osobních údajů

1. Družstvo dbá, aby při zpracování osobních údajů byly dodržovány následující zásady:
   a. **Zákonnost, korektnost, transparentnost:** Zpracovávat osobní údaje je možné pouze korektním, zákonným a transparentním způsobem, a to pouze na základě právních titulů definovaných v těchto Zásadách. Správci je uložena povinnost zajišťovat v co největší míře informovanost subjektů údajů a postupovat při zpracování osobních údajů otevřeně a v souladu s GDPR.
   b. **Účelové omezení:** Účel zpracování osobních údajů určuje rámec operací, které lze v daném účelu zpracování provádět. Vymezení účelu je přitom klíčovou povinností správce. Je zakázáno zpracovávat osobní údaje za jinými účely, než za kterými byly shromážděny. Z tohoto existují výjimky (např. pokud k tomu dá subjekt údajů souhlas, pokud je nový účel zpracování slučitelný s původním apod.). Zpracování za jinými účely je tzv. dalším zpracováním.
   c. **Minimalizace údajů:** Zpracovávají a shromažďují se pouze ty osobní údaje, které jsou relevantní a přiměřené vzhledem k účelu zpracování, a pouze v takovém rozsahu, který je nezbytný pro naplnění vymezeného účelu. Pokud by bylo možné dosáhnout účelu i bez zpracování některých osobních údajů, je nutné tyto nadbytečné osobní údaje přestat zpracovávat (např. pokud je správce schopen ztotožnit subjekt údajů i bez rodného čísla apod.).
   d. **Přesnost:** Zpracované údaje musí být přesné a musí odpovídat skutečnosti a v případě potřeby (dle povahy daného zpracování) je správce povinen provádět jejich aktualizaci. Jakmile správce či zpracovatel zjistí, že údaje jsou nepřesné, přijme veškerá rozumná opatření k tomu, aby nepřesné údaje opravil nebo zlikvidoval. Přesnost musí být zajišťována v průběhu zpracování i shromažďování údajů v rozsahu rizika případné újmy subjektu údajů. Subjektům údajů musí být uložena povinnost hlásit případné změny dříve uvedených osobních údajů. Správce neodpovídá za nepřesnost údaje, pokud mu subjekt údajů poskytne údaj nepravdivý.
   e. **Omezení a forma uložení:** Osobní údaje se uchovávají pouze po dobu, která je nezbytná pro účely, pro které jsou osobní údaje zpracovávány. Po skončení této doby se správci ukládá povinnost osobní údaje zlikvidovat (vymazat či anonymizovat), to neplatí, pokud je dána některá z výjimek stanovených v GDPR. Osobní údaje jsou uchovávány ve formě, která neumožňuje přístup neoprávněných osob k těmto údajům.
   f. **Integrita a důvěrnost:** Osobní údaje se zpracovávají takovým způsobem, který zajistí jejich zabezpečení před neoprávněným či protiprávním zpracováním a dále také zničením, poškozením či ztrátou apod.

2. Za účelem naplnění zásady odpovědnosti je nutné každému jednotlivému zpracování osobních údajů stanovit odpovědnou osobu stanovenou konkrétní pracovní pozicí. Tuto odpovědnou osobu určí osoba zastávající pracovní pozici, která je odpovědná za vedení registru zpracování.

IV. Povinnost mlčenlivosti

1. Každý, kdo se jakýmkoli způsobem podílí na zpracování osobních údajů nebo s nimi přichází do styku, či se o nich jakkoliv jinak dozví, je povinen zachovávat o těchto údajích mlčenlivost. To neplatí, pokud se jedná o informace jinak zveřejněné, nebo pokud to ukládají právní předpisy. Povinnost mlčenlivosti trvá také po ukončení pracovněprávního vztahu. Podrobnosti stanoví pracovní smlouva, případně další smlouvy (např. s externími zpracovateli osobních údajů apod.).

V. Právní tituly

1. Zpracování osobních údajů probíhá vždy na základě některého právního titulu uvedeného v čl. V. odst. 3. těchto Zásad. Bez právního titulu nelze osobní údaje zpracovávat, resp. jednalo by se o zpracování nezákonné.
2. Právní titul musí být stanoven nejpozději spolu s účelem daného zpracování. Právní titul navrhne osoba odpovědná za dané zpracování, která pak také existenci právního titulu průběžně sleduje.
3. Osobní údaje lze zpracovávat vždy pouze v odpovídajícím rozsahu a pouze na základě některého z těchto právních titulů:
   a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
   b) zpracování je nezbytné pro plnění smlouvy, jejíž stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
   c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
   d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby;
   e) 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;
   f) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce.
4. Na základě souhlasu subjektu údajů lze osobní údaje zpracovávat pouze v případě, že pro dané zpracování s ohledem na účel zpracování není možno využít jiný právní titul uvedený v odst. 3. písm. b) až f) tohoto článku. Souhlas jako právní titul daného zpracování tedy může být užit pouze v případě, kdy není možné použít žádný jiný právní titul.

5. Pod právní titul uvedený v odst. 3. písm. b) tohoto článku *(tj. „zpracování je nezbytné pro plnění smlouvy, jejíž stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů“)* lze podřadit pouze uzavření či plnění smluvního závazku. Aby mohl být tento právní titul využit, musí být stranou dané smlouvy sám subjekt údajů, anebo žádost o uzavření smlouvy musela vzejít přímo od subjektu údajů. Tento právní titul se nevztahuje na zpracování osobních údajů v důsledku nesplnění závazku.
6. Na základě právního titulu uvedeného v odst. 3. písm. c) tohoto článku (*tj. „zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje“*) lze zpracovávat osobní údaje pouze v případě povinnosti stanovené evropským či tuzemským právním předpisem natolik určitě, že z ní lze určit, jaké zpracování má být prováděno a správce (zpracovatel) nemá na výběr, jak a zda tuto povinnost splní.
7. Na základě právního titulu uvedeného v odst. 3. písm. d) tohoto článku *(tj. „zpracování je nezbytné pro ochranu životně důležitých zájmů subjektů údajů nebo jiné fyzické osoby“)* lze zpracovávat osobní údaje jedině tehdy, pokud je zpracování nutné k předejití vzniku újmy subjektu údajů či třetí osoby na zdraví či životě.
8. V případě zpracování osobních údajů na základě právního titulu uvedeného v odst. 3. písm. e) tohoto článku (tj. *„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“)* musí být před zahájením zpracování osobních údajů provedeno tzv. komplexní posouzení.

   Komplexní posouzení se skládá z těchto kroků:

   a) Definování oprávněného zájmu.
   b) Posouzení kritéria nezbytnosti (tj. posouzení, zda nelze sledovaného cíle dosáhnout jinými, méně invazivními prostředky).
   c) Balanční test.

   Balanční test se skládá z následujících kroků:

   a) Posouzení váhy oprávněného zájmu

   - zájmy správce vč. základních práv a svobod (svoboda projevu, podnikání apod.), vždy je však třeba zkoumat, zda je zpracování nezbytné a proporcionální
   - veřejné zájmy a zájmy komunity – veřejnosti (dobročinné činnosti, odhalování korupce, předcházení podvodům) - jeho existence může posílit oprávněný zájem správce a přidat mu na váze
   - ostatní oprávněné zájmy (subjektivní zájmy správce, síťová bezpečnost, přímý marketing)
   - právní, kulturní nebo společenské uznání oprávněného zájmu – jeho existence je schopná přidat na váze oprávněnému zájmu správce

b) Posouzení důsledků zpracování pro subjekty

- veškerá přímá i nepřímá újma, které může vzniknout, ale i emociální dopad (např. stres ze ztráty kontroly nad osobními údaji apod.)
- identifikace a nutnost zhodnotit pozitivní i negativní dopady kvantitativně, ale zejména kvalitativně
- nejen újma, kterou způsobí správce sám, ale i jednáním třetí osoby (po předání apod.)

c) Vyvážení zájmu s důsledky, které může zpracování na subjekt mít

- nutno vážit zájmy
- váží se i výhoda oproti pravděpodobnosti a velikosti újmy
- výsledkem by ideálně mělo být, že zájem subjektu údajů nepřevýší zájmy správce, tedy že výhody převáží dopad do práv a svobod subjektu údajů

d) Posouzení dostatečnosti plánovaných opatření a záruk

- při provádění testu je nezbytné vzít v úvahu opatření, která má správce v plánu provést podle GDPR (účelové omezení apod.)
- nejistý až neuspokojivý výsledek testu je možné zvrátit přijetím dodatečných záruk, díky kterým oprávněný zájem správce nakonec převáží nad zájmy subjektu údajů
- čím významnější je dopad zpracování na subjekt údajů, tím větší musí být věnována pozornost relevantním zárukám.

9. Osobní údaje smí být z titulu oprávněných zájmů správce či třetí strany uvedeného v odst. 3. písm. e) tohoto článku zpracovávány jedině tehdy, když na základě komplexního posouzení a balančního testu bude zjištěno, že zájmy nebo základní práva a svobody subjektu údajů nepřeváží nad oprávněnými zájmy správce či třetí strany. V případě neuspokojivého výsledku balančního testu je nutné přijmout další opatření k nápravě nedostatků a test opakovat nebo od záměru zpracování osobních údajů upustit. Dokud nebude výsledek balančního testu uspokojivý, nelze osobní údaje z titulu oprávněných zájmů správce či třetí strany zpracovávat.
10. Komplexní posouzení včetně balančního testu musí být provedeno ještě před zahájením zpracování z titulu oprávněných zájmů správce či třetí strany. O provedení komplexního posouzení a balančního testu se vyhotoví písemný záznam, který obsahuje popis a výsledek provedení jednotlivých kroků. Komplexní posouzení včetně balančního testu a vyhotovení záznamu o tomto komplexním posouzení provede vedoucí oddělení rizik a prevence. U již prováděných zpracování je tato osoba povinna vyhotovit komplexní posouzení bez zbytečného odkladu po přidělení této odpovědnosti.

VI. Účely zpracování osobních údajů

1. Každému zpracování osobních údajů musí být stanoven určitý, výslovně vyjádřený a legitimní účel. Účel nesmí být stanoven obecně a neurčitě. Účel musí být stanoven natolik určitě, aby z něj bylo patrné, jaká konkrétní zpracování na základě něj budou probíhat.
2. Bez stanovení určitého, výslovně vyjádřeného a legitimního účelu nelze osobní údaje zpracovávat.
3. Účel musí být stanoven nejpozději při shromažďování osobních údajů. Účel navrhne osoba odpovědná za dané zpracování. Za průběžné sledování existence účelu je odpovědná osoba odpovědná za dané zpracování.
4. Osobní údaje lze pro určitý účel zpracovávat pouze v nezbytném rozsahu a po nezbytně dlouhou dobu. Pokud není po uplynutí nezbytně dlouhé doby prováděno další zpracování za účelem slučitelným s původním účelem, nelze osobní údaje dále zpracovávat a musí být zlikvidovány.
5. Má-li dojít ke zpracování osobních údajů za jiným účelem, než ke kterému byly osobní údaje původně shromážděny (dále jen „*další zpracování*“), může být takové další zpracování založeno na souhlasu subjektu údajů nebo právu členského státu či Unie. Pokud další zpracování není založeno na souhlasu subjektu údajů nebo na právu Unie či členského státu, resp. není-li další zpracování nezbytné a přiměřené pro splnění povinnosti, která je správci uložena, musí být za účelem zjištění přípustnosti dalšího zpracování provedeno ze strany správce tzv. posouzení slučitelnosti účelů, které musí být provedeno před zahájením dalšího zpracování.
6. V rámci posouzení slučitelnosti účelů jsou zvažovány zejména tyto otázky:
   - jakákoli vazba mezi účely, kvůli nimž byly osobní údaje shromážděny, a účely zamýšleného dalšího zpracování;
   - okolnosti, za nichž byly osobní údaje shromážděny, zejména pokud jde o vztah mezi subjekty údajů a správcem;
   - povaha osobních údajů, zejména zda jsou zpracovávány zvláštní kategorie osobních údajů nebo osobní údaje týkající se rozsudků v trestních věcech a trestných činů;
   - možné důsledky zamýšleného dalšího zpracování pro subjekty údajů;
   - existence vhodných záruk (např. šifrování nebo pseudonymizace).
7. Další zpracování, které je posuzováno v rámci testu slučitelnosti účelů, smí být provedeno jedině tehdy, pokud účel dalšího zpracování v posouzení slučitelnosti účelů obstojí a bude vyhodnocen jako slučitelný s původním účelem.
8. Posouzení slučitelnosti účelů provádí a záznam o tomto posouzení vyhotovuje vedoucí oddělení rizik a prevence a to před zahájením dalšího zpracování. Družstvo je povinno o tomto dalším zpracování informovat subjekty údajů; o kladném výsledku testu slučitelnosti informuje osoba uvedená v tomto odstavci osobu odpovědnou za plnění informační povinnosti.

VII. Společná ustanovení k právním titulům a účelům

1. Na zpracování osobních údajů pouze na základě právních titulů předpokládaných GDPR a za určitým, výslovně vyjádřeným a legitimním účelem dohlíží vedoucí oddělení rizik a prevence. Po provedení kontroly je tato osoba odpovědná za neprodlené stanovení dalšího postupu v případě zjištění nedostatků.
2. Písemný návrh znění účelu a právního titulu daného zpracování navrženého odpovědnou osobou za dané zpracování, který byl proveden na základě čl. V. odst. 2 a VI. odst. 3. těchto Zásad, předá tato osoba oddělení rizik a prevence. V případě, že by měl být osobní údaj k danému účelu zpracováván prostřednictvím informačního systému, předá oddělení rizik a prevence písemný návrh účelu a právního titulu oddělení informačních technologií k vyjádření. Oddělení informačních technologií zašle své vyjádření k návrhu účelu a právního titulu oddělení rizik a prevence nejpozději do 14 pracovních dnů. Oddělení rizik a prevence poté na základě vlastního uvážení stanoví účel a právní titul zpracování. Oddělení rizik a prevence je povinno při určování účelu a právního titulu zohlednit vyjádření oddělení informačních technologií, pokud však oddělení rizik a prevence dospěje k odlišnému závěru, není povinno se vyjádřením oddělení informačních technologií řídit.
3. Pro stanovení účelu a právního titulu na základě postupu dle odst. 2. tohoto článku Zásad provede oddělení rizik a prevence konzultaci s právníkem družstva. Takto stanovený účel a právní titul oddělení rizik a prevence oznámí osobě odpovědné za dané zpracování dle čl. III. odst. 2 Zásad a osobě odpovědné za vedení registru zpracování.
4. Zaznamená-li Družstvo, že dochází ke zpracování osobních údajů bez právního titulu nebo účelu, nebo že došlo ke změně právního titulu nebo účelu, oznámí se tato skutečnost neprodleně osobě odpovědné za dané zpracování, a není-li taková osoba nebo není zaměstnanci známa, pak vedoucímu oddělení rizik a prevence. Tato osoba je povinna neprodleně prověřit oznámení a v případě potvrzení pravdivosti oznámení neprodleně rozhodnout o dalším postupu a oznámit tuto skutečnost osobě odpovědné za vedení registru zpracování, případně dalším osobám (osobě odpovědné za likvidaci, osobě odpovědné za plnění informační povinnosti apod.).
5. V případě, že dojde při zpracování osobního údaje ke změně právního titulu či účelu zpracování, informuje osoba odpovědná za plnění informační povinnosti o této změně neprodleně subjekt údajů.
6. Právní titul i účel každého zpracování jsou uvedeny v registru zpracování, za jehož vedení odpovídá vedoucí oddělení rizik a prevence.
7. Pokud právní titul a/nebo účel daného zpracování osobních údajů odpadne či dojde k naplnění účelu, jsou zaměstnanci povinni informovat o této skutečnosti odpovědnou osobu daného zpracování, která zajistí, aby bylo zpracování příslušných osobních údajů okamžitě ukončeno a tyto údaje byly zlikvidovány.

VIII. Souhlas subjektu údajů se zpracováním osobních údajů

1. Má-li být zpracování osobních údajů založeno na souhlasu subjektu údajů, musí tento souhlas splňovat všechny náležitosti dle čl. 7 GDPR, zejména musí být svobodný, konkrétní, informovaný a jednoznačný. Nesplňuje-li souhlas požadavky dle čl. 7 GDPR, nelze na jeho základě osobní údaje zpracovávat. Souhlas může udělit pouze subjekt údajů, který dovršil osmnáctý rok svého věku.
2. Aby mohl souhlas sloužit jako právní titul pro zpracování osobních údajů, musí být udělen písemně či elektronicky a musí být oddělen od ostatních skutečností, tedy musí tvořit samostatný dokument (tedy nesmí být například součástí obchodních podmínek).
3. Před udělením souhlasu je subjekt údajů informován o všech skutečnostech a okolnostech zpracování, aby byl souhlas skutečně informovaný. Zejména je subjekt údajů obeznámen s:
   a) totožností správce,
   b) účelem zpracování,
   c) operacemi zpracování a jejich důsledky pro subjekt údajů,
   d) možností souhlas kdykoli odvolat.
4. Vzorový souhlas subjektu údajů se zpracováním osobních údajů je možno získat na žádost.
5. Souhlas subjektu údajů se zpracováním osobních údajů je archivován po celou dobu zpracování osobních údajů vedoucím příslušného oddělení, který musí být jeho prostřednictvím schopen kdykoliv prokázat všechny skutečnosti každého souhlasu dle odst. 6. tohoto článku.
6. Ke každému souhlasu je evidováno:
   a) kdo je subjektem údajů,
   b) kdy byl souhlas udělen,
   c) k jakému zpracování a pro jaký účel byl souhlas udělen,
   d) jaké informace měl subjekt údajů k dispozici před udělením souhlasu,
   e) v jaké formě byl souhlas udělen a jaký byl jeho obsah,
   f) údaj o tom, zda a případně kdy byl souhlas odvolán.
7. Po uplynutí doby, na níž byl souhlas udělen, nebo poté, co byl souhlas odvolán, musí být souhlas i osobní údaje, k jejichž zpracování byl souhlas udělen, bez zbytečného odkladu zlikvidovány (vymazány nebo anonymizovány). Výmaz nebude proveden pouze u těch osobních údajů, které jsou dále zpracovávány na základě jiného právního titulu.
8. V případě odvolání souhlasu je dokument, v němž subjekt údajů svůj souhlas odvolává bez zbytečného odkladu předán osobě odpovědné za dané zpracování, která prostřednictvím informování příslušných osob (osoby odpovědné za plnění informační povinnosti, likvidaci apod.) zajistí, aby bylo zpracování příslušných osobních údajů okamžitě ukončeno a tyto údaje byly zlikvidovány a aby byly neprodleně vyzváni k likvidaci těchto osobních údajů také všichni zpracovatelé, kterým byly osobní údaje předány.

IX. Obecně k právům subjektů údajů a komunikaci s nimi

1. Vedoucí oddělení rizik a prevence odpovídá za dodržování způsobu komunikace se subjekty údajů, za plnění informační a oznamovací povinnosti vůči subjektům údajů a jiným externím subjektům a vyřizování veškerých žádostí subjektů údajů. Osoba uvedená v předchozí větě spolupracuje zejména s osobami odpovědnými za dané zpracování a osobou odpovědnou za vedení registru zpracování.
2. Vedoucí oddělení rizik a prevence musí se subjekty údajů komunikovat a informace jim sdělovat stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků. Takové komunikace lze dosáhnout např. strukturováním textu, užíváním jednoduchých vět a nikoliv odborných termínů, využití grafů či jiných grafických prvků apod.
3. Vedoucí oddělení a prevence musí přijmout vhodná opatření, aby se na něho subjekt údajů mohl obrátit alespoň:
   a) písemně (poštou),
   b) elektronicky (např. přes webový formulář) a
   c) ústně (osobní návštěvou nebo telefonicky).
4. Způsob komunikace musí být zvolen tak, aby byl vhodný a přiměřený okolnostem zpracování. Správce musí respektovat způsob komunikace zvolený subjektem údajů. Informační povinnost dle čl. X., XI. a XII. Směrnice může správce plnit také zveřejněním způsobem umožňujícím dálkový přístup.
5. Veškerá komunikace (vč. jejího obsahu a doby jejího provedení) se subjekty údajů musí být zaznamenána pro účely jejího pozdějšího doložení. Za toto doložení je odpovědný vedoucí oddělení rizik a prevence.

X. Informační povinnost v případě získání osobních údajů přímo od subjektu údajů

1. V případě, kdy správce získává osobní údaje přímo od subjektu údajů (sdělí mu je osobně, telefonicky, vyplní žádost apod.), musí být subjektu údajů v okamžiku získání těchto osobních údajů poskytnuty alespoň následující informace:
   a) totožnost a kontaktní údaje správce a jeho zástupce ve věcech ochrany osobních údajů;
   b) kontaktní údaje pověřence pro ochranu osobních údajů, byl-li v Družstvu jmenován;
   c) účely zpracování, pro které jsou osobní údaje určeny, a právní titul pro zpracování;
   d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na právním titulu oprávněného zájmu;
   e) příjemce nebo kategorie příjemců osobních údajů;
   f) způsob a rozsah zpracování a případné dopady tohoto zpracování do práv a svobod subjektů údajů;

g) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
h) existence a způsob uplatnění práva požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů;
i) pokud je zpracování založeno na souhlasu subjektu údajů, existence práva odvolat kdykoli souhlas, aniž by tím byla dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
j) existenci práva podat stížnost u dozorového úřadu;
k) skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;
l) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

2. Informace dle předchozího odstavce nemusí být subjektu údajů poskytnuty, pokud je správce schopen prokázat, že tyto informace subjekt údajů již má, a do té míry, v níž je má. V případě výslovné žádosti subjektu údajů však musí být informace poskytnuty i opětovně.

XI. Informační povinnost v případě získání osobních údajů jinak než od subjektu údajů

1. Jestliže osobní údaje nebyly získány přímo od subjektu údajů, poskytne správce subjektu údajů tyto informace:
   a) informace uvedené v čl. X. odst. 1. Zásad, a to kromě informací dle čl. X. odst. 1. písm. k) Zásad;
   b) kategorie osobních údajů, o jejichž získání a zpracovávání správce informuje;
   c) zdroj osobních údajů.
2. Informace dle předchozího odstavce musí být poskytnuty v následujících lhůtách:
   a) bez zbytečného odkladu, a to nejpozději do jednoho měsíce od získání osobních údajů;
   b) v případě navázání komunikace se subjektem údajů, nejpozději v okamžiku, kdy poprvé dojde k uvedené komunikaci;
   c) v případě zpřístupnění osobních údajů jinému příjemci, nejpozději při prvním takovém zpřístupnění osobních údajů.
3. Informace dle odst. 1. nemusí být subjektu údajů poskytnuty v následujících případech:
   a) správce je schopen prokázat dřívější poskytnutí informací subjektu údajů; v případě výslovné žádosti subjektu údajů však musí být informace poskytnuty i opětovně;
   b) poskytnutí informací není možné nebo by vyžadovalo nepřiměřené úsilí (např. pokud nejsou známy kontaktní údaje subjektů údajů a tyto kontaktní údaje je nemožné nebo velmi obtížné získat);

c) poskytnutí informací by zmařilo cíl daného zpracování (např. odhalení podvodu apod.);
d) získávání nebo zpřístupnění osobních údajů je výslovně stanoveno právním řádem;
e) osobní údaje jsou správcem zpracovávány jako důvěrné a všechny osoby, které s nimi přijdou do styku, jsou povinny zachovávat služební nebo profesní tajemství, včetně zákonné povinnosti mlčenlivosti.

XII. Informační povinnost v případě dalšího zpracování

1. Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před dalším zpracováním informace o tomto jiném účelu a dále;
   a) informace uvedené v čl. X. odst. 1. Zásad, pokud byly osobní údaje získány přímo od subjektu údajů, nebo
   b) informace uvedené v čl. XI. odst. 1. Zásad, pokud osobní údaje nebyly získány přímo od subjektu údajů.
2. Informace dle předchozího odstavce nemusí být subjektu údajů poskytnuty v případech
   a) uvedených v čl. X. odst. 2. Zásad, pokud byly osobní údaje získány přímo od subjektu údajů, nebo
   b) uvedených v čl. XI. odst. 3. Zásad, pokud osobní údaje nebyly získány přímo od subjektu údajů.

XIII. Oznamovací povinnost vůči příjemcům osobních údajů

1. Vedoucí oddělení rizik a prevence oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování, s výjimkou případů, kdy se to ukáže jako nemožné nebo to vyžaduje nepřiměřené úsilí.
   Je-li správce povinen oznámit příjemci provedenou opravu, omezení zpracování nebo výmaz osobních údajů, může tak učinit změnou osobních údajů v evidenci, pokud příjemci pravidelně zpřístupňuje její platný obsah.
2. Vedoucí oddělení rizik a prevence informuje subjekt údajů o příjemcích dle čl. X. odst. 1. a čl. XI. odst. 1. Zásad.

XIV. Práva subjektů údajů

1. Vedoucí oddělení rizik a prevence stanoví jednoduché postupy, jak se na správce mohou subjekty údajů obracet za účelem uplatnění svých práv. Dále je tato osoba povinna v rámci informační povinnosti aktivně upozorňovat, případně zajistit aktivní upozornění subjektů údajů o jejich právech a o tom, jak a kde je mohou uplatňovat.

2. Při vyřizování žádostí i při informování subjektů údajů o postupech vyřizování žádostí musí být vždy dodrženy zásady komunikace se subjekty údajů uvedené v čl. X. až XIII. Zásad. Postup při vyřizování žádostí, včetně odůvodnění způsobu vyřízení žádosti, musí být zaznamenán.

XV. Identifikace subjektů údajů

1. Před vyřízením každého uplatněného práva musí být bezpečně identifikován subjekt údajů tak, aby neoprávněná osoba nemohla získat, smazat či pozměnit osobní údaje jiného subjektu údajů.
2. Konkrétní způsoby identifikace subjektů údajů musí být stanoveny individuálně, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody subjektů údajů. Požadavky na ověření totožnosti je možno stanovit dle konkrétních uplatněných práv (např. u žádosti o potvrzení o zpracování údajů je riziko nižší než u žádosti o poskytnutí kopie údajů. Z toho důvodu může být u prvního druhu žádosti vyžadovány nižší nároky na ověření totožnosti subjektu údajů apod.).
3. Pokud nelze subjekt údajů bezpečně identifikovat na základě jím poskytnutých údajů, může být po subjektu údajů požadováno poskytnutí dalších dodatečných údajů. Nesmí však být vyžadovány identifikační údaje, které nejsou pro provedení identifikace nezbytné.
4. Pokud nelze subjekt údajů jednoznačně identifikovat ani podle předchozího odstavce, může být vyřízení žádosti odepřeno, o čemž musí být subjekt údajů informován.

XVI. Lhůta pro vyřízení žádosti subjektů údajů a způsoby jejího vyřízení

1. Bez zbytečného odkladu, nejpozději však do jednoho měsíce od obdržení žádosti subjektu údajů musí být žádosti vyhověno, nebo žádost odmítnuta.
2. Žádosti je vyhověno, pokud jsou provedena požadovaná opatření a subjekt údajů je o těchto opatřeních informován, případně pokud je subjekt údajů informován o skutečnostech, o které žádal apod.
3. Žádost je odmítnuta, pokud je odmítnuto provedení požadovaných opatření a subjekt údajů je informován o důvodech takového odmítnutí spolu s poučením o možnosti podat stížnost u dozorového úřadu a o možnosti žádat soudní ochranu.
4. Prodloužit lhůtu pro vyhovění žádosti je možné v případě potřeby a s ohledem na složitost a počet žádostí až o dva měsíce. Subjekt údajů musí být informován o prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad.
5. Žádosti může být vyhověno i zčásti. Ve zbylé části musí být žádost odmítnuta.

XVII. Poplatky za vyřízení žádosti

1. Vyřizování žádostí je zásadně bezplatné. Poplatky spojené s vyřízením žádosti mohou být požadovány pouze výjimečně.
2. Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené může být:
   a) uložen přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů; nebo
   b) odmítnuto žádosti vyhovět.
3. Zjevně nedůvodnou je zejména taková žádost, která zcela postrádá odůvodnění (pokud je odůvodnění nezbytné), nebo z jejího obsahu nelze ani výkladem dovodit, o co subjekt údajů žádá.
4. Nepřiměřenými jsou také žádosti, které se opakují, aniž by k tomu byl oprávněný důvod.
5. Zjevnou nedůvodnost nebo nepřiměřenost musí být správce schopen doložit.

XVIII. Právo na přístup

1. Subjekt údajů má zejména právo požadovat po správci,
   a) aby mu poskytl informaci o tom, zda zpracovává osobní údaje, které se ho týkají, a /nebo
   b) aby mu případně zpracovávané osobní údaje zpřístupnil.
2. Na žádost subjektu údajů mu musí být poskytnuty následující informace:
   a) informace (potvrzení) o tom, zda správce zpracovává osobní údaje;
   b) kopie zpracovávaných osobních údajů;
   c) informace o zpracováních prováděných v minulosti;
   d) účely zpracování;
   e) kategorie dotčených osobních údajů;
   f) příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
   g) plánovaná doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
   h) existence práva požadovat od správce opravu nebo výmaz osobních údajů týkajících se subjektu údajů nebo omezení jejich zpracování anebo vznést námitku proti tomuto zpracování;
   i) právo podat stížnost u dozorového úřadu;
   j) veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů;
   k) skutečnost, že dochází k automatizovanému rozhodování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.
3. Žádost může být subjektem údajů omezena pouze na některé informace. Pokud však žádost omezena nebude, je nutné poskytnout všechny informace a údaje.

4. Zpřístupněním údajů dle odst. 1. písm. b) tohoto článku se rozumí poskytnutí kopie zpracovávaných osobních údajů. Poskytnutí první kopie zpracovávaných osobních údajů je vždy bezplatné. Bezplatné je také poskytnutí kopie po každé změně osobních údajů nebo po uplynutí doby, za kterou lze důvodně očekávat změnu osobních údajů.
5. Kopie zpracovávaných osobních údajů nebudou poskytnuty, jestliže by tím byla nepříznivě dotčena práva a svobody jiných osob.

XIX. Právo na opravu

1. Subjekt údajů má právo požadovat:
   a) opravu jeho nepřesných osobních údajů a/nebo
   b) doplnění jeho neúplných osobních údajů.
2. V případě, že subjekt údajů podá žádost dle odst. 1 písm. a) tohoto článku, musí správce bezodkladně ověřit, zda jsou osobní údaje skutečně nepřesné, a po tuto dobu omezit zpracování dotčených osobních údajů.
3. V případě, že subjekt údajů podá žádost dle odst. 1 písm. b) tohoto článku, doplní správce požadované údaje pouze, pokud je to vhodné vzhledem k účelu zpracování. Správce nesmí provést požadované rozšíření, pokud subjektem údajů doplňované údaje není nezbytné zpracovávat vzhledem k danému účelu.

XX. Právo na výmaz

1. Subjekt údajů má právo na vymazání (zlikvidování) svých osobních údajů a správce je povinen osobní údaje bez zbytečného odkladu vymazat, pokud je dán alespoň jeden z následujících důvodů:
   a) osobní údaje nejsou potřeba pro účel, pro který jsou zpracovávány;
   b) osobní údaje jsou zpracovávány výhradně na základě souhlasu a subjekt údajů odvolá souhlas s jejich zpracováním a neexistuje žádný další právní titul pro zpracování;
   c) subjekt údajů vznese námitku proti zpracování a při jejím posouzení vyjde najevo, že neexistují žádné převažující oprávněné důvody pro zpracování, nebo v případě zpracovávání osobních údajů pro účely přímého marketingu subjekt údajů vznese námitku proti tomuto zpracování;
   d) osobní údaje byly zpracovány protiprávně;
   e) na správce se vztahuje povinnost vyplývající z právního řádu, která mu ukládá osobní údaje vymazat;
   f) jedná se o osobní údaje dětí shromážděné správcem v souvislosti s nabídkou služby informační společnosti.
2. I v případě, že je dán některý z důvodů dle odst. 1. tohoto článku, může správce osobní údaje dále zpracovávat, pokud je zpracování nezbytné:
   a) pro výkon práva na svobodu projevu a informace;

b) pro splnění právní povinnosti správce, jež vyžaduje zpracování podle právního řádu, nebo pro splnění úkolu správce provedeného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen;
c) z důvodů veřejného zájmu v oblasti veřejného zdraví;
d) pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely, pokud je pravděpodobné, že by právo na výmaz znemožnilo nebo vážně ohrozilo splnění cílů uvedeného zpracování;
e) pro určení, výkon nebo obhajobu právních nároků.

3. Za splnění povinnosti dle tohoto článku odpovídá vedoucí oddělení rizik a prevence.

XXI. Právo na omezení zpracování

1. Subjekt údajů má právo na omezení zpracování svých osobních údajů v těchto případech:
   a) subjekt údajů popírá přesnost osobních údajů, a to na dobu potřebnou k tomu, aby správce mohl přesnost osobních údajů ověřit;
   b) zpracování je protiprávní a subjekt údajů odmítá výmaz osobních údajů a žádá místo toho o omezení jejich použití;
   c) správce již osobní údaje nepotřebuje pro účely zpracování, ale subjekt údajů je požaduje pro určení, výkon nebo obhajobu právních nároků;
   d) subjekt údajů vznesl námitku proti zpracování a probíhá posouzení existence oprávněných důvodů pro zpracování.
2. Osobní údaje, jejichž zpracování bylo omezeno, nelze zpracovávat jinak než jejich uložením. Během trvání omezení zpracování tak nelze dotčené osobní údaje ani zlikvidovat.
3. Musí být stanovena konkrétní technická řešení omezení zpracování (např. jejich označení v systému, znepřístupnění, dočasný přesun, dočasný výmaz apod.).
4. Jiné zpracování osobních údajů, jejichž zpracování bylo omezeno na pouhé uložení, je možné pouze:
   a) se souhlasem subjektu údajů,
   b) z důvodu určení, výkonu nebo obhajoby právních nároků,
   c) z důvodu ochrany práv jiné fyzické nebo právnické osoby nebo
   d) z důvodu důležitého veřejného zájmu EU nebo některého členského státu.
5. O ukončení omezení zpracování musí být subjekt údajů předem informován.
6. Omezením zpracování osobních údajů není dotčena povinnost osobní údaje předat nebo zpřístupnit, je-li tato povinnost stanovena právním předpisem. Tyto údaje se při předání nebo zpřístupnění označí jako údaje uvedené v čl. 18 odst. 1 GDPR.

XXII. Právo na přenositelnost

1. Subjekt údajů má právo:
   a) obdržet osobní údaje ve strojově čitelném formátu a
   b) požadovat přímé předání osobních údajů ve strojově čitelném formátu jinému správci, pokud je to technicky možné.
2. Strojově čitelným formátem se rozumí strukturovaný, běžně používaný a strojově čitelný formát, ve kterém jsou uloženy automatizovaně zpracovávané osobní údaje (např. formáty XML, JSON a CSV).
3. Práva uvedená v odst. 1 tohoto článku má subjekt údajů pouze vůči osobním údajům splňujícím následující podmínky:
   a) osobní údaje jsou zpracovávány automatizovaně,
   b) osobní údaje jsou zpracovávány na základě souhlasu nebo za účelem plnění smlouvy a
   c) osobní údaje byly poskytnuty přímo subjektem osobních údajů (např. také údaje vysledované na základě využívání služby nebo zařízení příslušným subjektem).
4. Osobní údaje ve strojově čitelném formátu nebudou poskytnuty ani předány, jestliže by tím byla nepříznivě dotčena práva a svobody jiných osob.

XXIII. Právo vznést námitku

1. Subjekt údajů má právo vznést námitku proti zpracování osobních údajů, které je prováděno:
   a) pro splnění úkolu ve veřejném zájmu nebo při výkonu veřejné moci,
   b) pro účely oprávněných zájmů správce či třetí strany,
   c) pro účely přímého marketingu nebo
   d) pro účely vědeckého či historického výzkumu nebo pro statistické účely.
2. V případě, že je vznesena námitka dle odst. 1 písm. a) nebo b) tohoto článku musí být učiněny následující kroky:
   a) bez zbytečného odkladu musí být omezeno zpracovávání dotčených osobních údajů za jiným účelem, než je určení, výkon nebo obhajoba právních nároků;
   b) musí být provedeno posouzení spočívající v tom, zda má správce pro další zpracovávání oprávněné důvody, které převáží nad zájmy a svobodami subjektu údajů (balanční test);
   c) v případě, že správce nemá oprávněné důvody pro dané zpracovávání dotčených osobních údajů, musí být příslušné zpracovávání osobních údajů ukončeno.
3. V případě, že je vznesena námitka dle odst. 1. písm. c) tohoto článku musí být bez zbytečného odkladu zpracovávání osobních údajů za účelem přímého marketingu ukončeno.
4. V případě, že je vznesena námitka dle odst. 1. písm. d) tohoto článku musí být bez zbytečného odkladu zpracovávání osobních údajů za účelem vědeckého či historického výzkumu nebo pro statistické účely ukončeno, ledaže je zpracování nezbytné pro splnění úkolu prováděného z důvodu veřejného zájmu.

XXIV. Záznamy o zpracování osobních údajů

1. Správce je povinen vést záznamy o jednotlivých činnostech zpracování, které se vyhotovují písemně (i elektronickou formou).
2. Vedoucí oddělení rizik a prevence odpovídá za vedení záznamů o činnostech zpracování osobních údajů. Tyto záznamy jsou uloženy na síťové jednotce GDPR (G:) po celou dobu daného zpracování osobních údajů. Po ukončení zpracování jsou záznamy o zpracování neprodleně zlikvidovány.
3. Záznamy o zpracování obsahují následující informace:
   a) jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;
   b) účely zpracování;
   c) popis kategorií subjektů údajů a kategorií osobních údajů;
   d) kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny;
   e) informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce GDPR doložení vhodných záruk;
   f) je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;
   g) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.

XXV. Posouzení rizik a posouzení vlivu na ochranu osobních údajů

1. Vedoucí oddělení rizik a prevence zabezpečuje posouzení rizik každého zpracování pro práva a svobody subjektu údajů.
2. V rámci posouzení rizik dle odst. 1. tohoto článku je nutné pro každé zpracování určit míru rizika v některém z těchto stupňů, které je nutné stanovit s přihlédnutím ke všem okolnostem zpracování:
   - nízké riziko
   - střední riziko
   - vysoké riziko.
3. V případě, že se jeví jako pravděpodobné, že určitý druh zpracování bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody fyzických osob, provede vedoucí oddělení rizik a prevence posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.
4. Posouzení vlivu na ochranu osobních údajů musí být provedeno zejména v těchto případech zpracování:
   a) 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;

b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 GDPR nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 GDPR;
c) rozsáhlé systematické monitorování veřejně přístupných prostorů.
d) zpracování, které dle *Seznamu druhů zpracování osobních údajů, které podléhají posouzení vlivu na ochranu osobních údajů*, vydaného Úřadem pro ochranu osobních údajů, posouzení vlivu na ochranu osobních údajů podléhá.

5. Odpovědná osoba uvedená provede posouzení vlivu na ochranu osobních údajů také u všech operací zpracování, která dozorový úřad zveřejní v seznamu operací zpracování, které podléhají posouzení vlivu na ochranu osobních údajů.
6. Posouzení vlivu na ochranu osobních údajů musí splňovat náležitosti dle čl. 35 GDPR a obsahovat alespoň:
   a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;
   b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;
   c) posouzení rizik pro práva a svobody subjektů údajů;
   d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.
7. Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést. Správce nemusí provádět posouzení vlivu ani tehdy, pokud dané zpracování v souladu se Seznamem druhů zpracování osobních údajů, které nepodléhají posouzení vlivu na ochranu osobních údajů, vydaným Úřadem pro ochranu osobních údajů, posouzení vlivu nepodléhá.

XXVI. Pravidla pro fyzické zabezpečení

1. Přítomnost třetích osob v prostorách Družstva (zejména v místnostech, kde jsou zpracovávány osobní údaje) může ohrozit bezpečnost zpracovávaných osobních údajů. Třetími osobami se kromě zákazníků prodejny rozumí zejména osoby vykonávající tyto činnosti:
   a. údržba technického či programového vybavení,
   b. konzultační činnost,
   c. úklidové, zásobovací, bezpečnostní a další služby.
2. Podmínky, za kterých může třetí osoba přistupovat do místností, kde jsou zpracovávány osobní údaje, či přímo k těmto osobním údajům musí být upraveny v písemné smlouvě.
3. Osobní údaje nesmějí být zpracovávány v prostorách, v nichž se mohou volně pohybovat zákazníci a další neoprávněné osoby. Jsou-li osobní údaje zpracovávány přímo v budově prodejny, musí toto zpracování probíhat v zabezpečené místnosti, kam nemá volný přístup veřejnost.

4. Přístup k osobním údajům mohou mít pouze zaměstnanci, jejichž přístup je nezbytný pro řádné plnění jejich povinností. Pokud zaměstnanec přístupem nedisponuje, a potřebuje k osobním údajům přistoupit, musí být jeho přístup schválen, případně evidován (např. zaznamenán do knihy apod.). Schválení nebo evidování přístupu musí být řádně vedeno a uloženo.
5. Přístup k počítačovým zařízením, aplikacím a informačním systémům musí být upraven tak, aby byl přístup umožněn jen oprávněným uživatelům.
6. Každá místnost musí poskytovat možnost ochrany (uzamčení) v ní se nalézajících osobních údajů, a to zejména po dobu, kdy v ní není přítomen žádný zaměstnanec. Vstupní dveře a zámky musí vykazovat určitý stupeň odolnosti vůči neoprávněnému vniknutí *(bezpečnostní zámky, mříže na nízko umístěných oknech apod.)*.
7. Referát správy nemovitostí zajistí, aby byly zaměstnanci přiděleny klíče od těch místností, do nichž má mít zaměstnanec s ohledem na jemu svěřené činnosti přístup. Zaměstnanci nesmí klíče bez svolení vedoucího předat další osobě. Náhradní klíče jsou uloženy na referátu správy nemovitostí a jejich použití je ze strany referátu správy nemovitostí evidováno.
8. Při ukončení pracovního poměru zajistí referát správy nemovitostí odebrání klíčů a případných dalších obdobných přístupových prostředků zaměstnance. Zaměstnanec je také povinen vrátit všechny dokumenty, které mohou obsahovat osobní údaje, vč. jejich kopií. Případně se zaměstnanec zaváže tyto kopie zlikvidovat.
9. Všechny místnosti jsou pravidelně podrobovány požární revizi. Místnosti, v nichž se zpracovávají osobní údaje, nebo jejich bezprostřední okolí jsou vybaveny prostředky, které minimalizují rozsah případného požáru (např. detektory kouře, protipožární dveře, hasicí přístroje apod.).
10. Veškeré dokumenty obsahující osobní údaje musí být po dobu, kdy se nepoužívají, uzamčeny v uzamykatelných zásuvkách či jiném bezpečném druhu nábytku či jinak zabezpečeny. To platí především tehdy, není-li v místnosti, v níž se dokument nachází, přítomen oprávněný zaměstnanec.
11. Zaměstnanci nesmí v době své nepřítomnosti na pracovišti zanechávat volně přístupná (např. v kancelářích na stolech, na kopírkách v kancelářích či na chodbách, v prodejní části budovy apod.) jakákoli elektronická či neelektronická média s osobními údaji či nezabezpečené počítače.
12. Zaměstnanec si nesmí ukládat žádné dokumenty obsahující osobní údaje na plochu svého počítače a při odchodu z kanceláře je zaměstnanec povinen svůj počítač uzamknout.
13. Zaměstnanci jsou povinni chránit dokumenty uložené ve svých počítačích unikátním heslem, které nesmí sdělit žádné další osobě.

XXVII. Docházka a docházkový systém, hlídací služba

1. Každému zaměstnanci je při přijetí do pracovního poměru, po podpisu pracovní smlouvy a zadání údajů v systému SAP, přidělen jedinečný číselný kód (osobní číslo zaměstnance), který se přiřadí v databázi docházkového systému zaměstnanci. Za zadání číselného kódu do systému odpovídá zaměstnanec oddělení lidských zdrojů.
2. Při ukončení pracovního poměru zajistí zaměstnanec oddělení lidských zdrojů odebrání přístupových oprávnění v docházkovém terminálu.

XXVIII. Monitoring prostřednictvím kamerového systému, GPS, monitoring navštívených webových stránek zaměstnanci a správa internetových stránek

1. V prostorách Družstva je provozován kamerový systém.
2. Družstvo monitoruje vymezené prostory, a to zejména na pracovišti za účelem ochrany práv a právem chráněných zájmů Družstva, zaměstnanců i třetích osob. Družstvo monitoruje vymezené prostory za účelem ochrany svého majetku před protiprávním jednáním (odcizením, poškozením, zneužitím apod.) a ochrany majetku a zdraví zaměstnanců a dalších osob.
3. Jednotlivé kamery snímají vstupní prostory, prostory prodejních ploch, zejména jejich zadní části a části, které jsou obtížně sledovatelné personálem prodejny, dále prostory skladů, kde dochází k vykládce zboží, a vchodů do těchto prostor.
4. Záznamy kamerového systému jsou Družstvem uchovávány po dobu 7 dnů, což je nezbytná doba, která slouží k případnému odhalení konkrétního protiprávního jednání.
5. Využití kamerového systému v prostorách sloužících výhradně k soukromým účelům zaměstnanců či jiných osob (např. toalety, šatna) je zakázáno.
6. O přístupu k záznamům kamerového systému jsou pořizovány záznamy, na základě kterých lze identifikovat, kdy, kým a z jakého důvodu byly osobní údaje z kamerového systému zpracovány.
7. Za správu záznamů z kamerových systémů i záznamů o přístupu k nim odpovídají pověření zaměstnanci oddělení informačních technologií.
8. Prostory, které jsou monitorovány, musí být viditelně označeny nápisem *„Prostor je monitorován kamerovým systémem“* a příslušným piktogramem.
9. Podrobnosti ohledně provozování kamerového systému stanoví zvláštní vnitřní předpis.
10. Údaje GPS využívá pověřená osoba odboru logistiky a dopravy pro změny v plánu, a to pro maximální vytížení vozidel.
11. Kontrolu využití vozidel provádí dle GPS a Knihy jízd pověřená osoba oddělení rizik a prevence.
12. Podrobnosti ohledně využití GPS stanoví zvláštní vnitřní předpis.
13. Monitoring navštívených webových stránek provádí pověření zaměstnanci oddělení informačních technologií.

14. Oprávnění ke správě internetových stránek Družstva mají pracovníci oddělení marketingu a pověření zaměstnanci oddělení informačních technologií.

XXIX. Školení zaměstnanců

1. Za účelem zajišťování souladu s GDPR přijímá Správce veškerá potřebná opatření, jejichž součástí jsou úvodní, případně následná školení všech zaměstnanců Družstva. Cílem školení je informovat zaměstnance o jejich povinnostech tak, aby jejich činnost odpovídala požadavkům GDPR.

XXX. Ohlašování případů porušení zabezpečení

1. Dozví-li se zaměstnanec Družstva o případu porušení zabezpečení osobních údajů zpracovávaných v rámci Družstva, oznámí tuto skutečnost neprodleně výkonnému řediteli. V případě, že se jeví jako pravděpodobné, že toto porušení může mít za následek riziko pro práva a svobody fyzických osob, ohlásí odpovědná osoba dle předchozí věty porušení zabezpečení osobních údajů dozorovému úřadu, a to nejpozději do 72 hodin, od okamžiku, kdy se o porušení dozvěděl. Pokud dané porušení neohlásí v této lhůtě, musí připojit k ohlášení též důvody tohoto zpoždění.
2. Pokud bude vyhodnoceno, že je nepravděpodobné, že porušení dle odst. 1 tohoto článku může mít za následek riziko pro práva a svobody fyzických osob, a tedy nebude porušení oznámeno dozorovému úřadu, je výkonný ředitel povinen zdokumentovat důvody tohoto neoznámení, resp. vysvětlení, proč nemá porušení za následek riziko pro práva a svobody fyzických osob.
3. Ohlášení podle odst. 1 tohoto článku obsahuje především tyto informace:
   a) popis povahy daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;
   b) jméno a kontaktní údaje pověřence pro ochranu osobních údajů nebo jiného kontaktního místa, které může poskytnout bližší informace;
   c) popis pravděpodobných důsledků porušení zabezpečení osobních údajů;
   d) 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.
4. Výkonný ředitel oznámí porušení zabezpečení osobních údajů bez zbytečných odkladů také subjektu údajů, jestliže je pravděpodobné, že takové porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Oznámení se provede za použití jasných a jednoduchých jazykových prostředků, které popíší povahu porušení zabezpečení osobních údajů a uvedou přijatá opatření.

5. Oznámení dle předchozího odstavce se nevyžaduje, pokud správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů se již pravděpodobně neprojeví nebo pokud by to vyžadovalo nepřiměřené úsilí. I to je nutné písemně zachytit a uchovat. Oznámení dle předchozího odstavce se provede v omezeném rozsahu nebo je odloženo, je-li to nezbytné a svým rozsahem přiměřené k zajištění chráněného zájmu uvedeného v § 6 odst. 2 zákona o zpracování OÚ[1]. O takovém postupu vedoucí oddělení rizik a prevence bez zbytečného odkladu vyrozumí Úřad pro ochranu osobních údajů.
6. Výkonný ředitel je povinen o veškerých porušeních zabezpečení osobních údajů vést dokumentaci, tedy i o těch, která nebyla hlášena nebo oznámena.

XXXI. Archivace a skartace osobních údajů

1. Osobní údaje se vždy uchovávají pouze po dobu, která je nezbytná k dosažení účelu jejich zpracování a po dobu trvání příslušného právního titulu. Osobní údaje musí být archivovány a likvidovány.
2. Osobou odpovědnou za likvidaci osobních údajů je vedoucí oddělení rizik a prevence, pokud k tomu nebude určena jiná osoba na základě zvláštního vnitřního předpisu Družstva.

XXXII. Zapojení externích subjektů do zpracovávání osobních údajů

1. Výkonný ředitel odpovídá za dodržování způsobu zapojení externích subjektů do zpracování osobních údajů dle těchto Zásad.
2. U jakéhokoliv externího subjektu, který bude zapojen do zpracování osobních údajů, musí být před tímto zapojením posouzeno, zda:
   a. externí subjekt stanovuje vlastní účely a prostředky zpracování, a zda je tak ve vztahu k příslušnému zpracování samostatným správcem; nebo
   b. správce a externí subjekt stanovují účely a prostředky zpracování společně, a zda jsou tak ve vztahu k příslušnému zpracování společnými správci; nebo zda
   c. externí subjekt zpracovává osobní údaje pro správce na základě pověření (pokynů) správce, a zda je tak ve vztahu k příslušnému zpracování zpracovatelem osobních údajů.

[1] Chráněným zájmem se v této souvislosti rozumí:
   a) obranné nebo bezpečnostní zájmy České republiky,
   b) veřejný pořádek a vnitřní bezpečnost, předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkon trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech,
   c) jiný důležitý cíl veřejného zájmu Evropské unie nebo členského státu Evropské unie, zejména důležitý hospodářský nebo finanční zájem Evropské unie nebo členského státu Evropské unie, včetně záležitostí měnových, peněžních, rozpočtových, daňových a finančního trhu, veřejného zdraví nebo sociálního zabezpečení,
   d) ochrana nezávislosti soudů a soudců,
   e) předcházení, vyhledávání, odhalování nebo stíhání porušování etických pravidel regulovaných povolání,
   f) dohledové, kontrolní nebo regulační funkce spojené s výkonem veřejné moci v případech uvedených v písmenech a) až e),
   g) ochrana práv a svobod osob, nebo
   h) vymáhání soukromoprávních nároků.

3. Společní správci musí mít mezi sebou uzavřenou písemnou smlouvu, ve které si proporcionálně rozdělí odpovědnost za plnění povinností vyplývajících z GDPR (zejména informační povinnost a povinnosti vztahující se k právům subjektů údajů). Při rozdělení odpovědnosti společných správců musí být zohledněny úlohy jednotlivých správců v rámci zpracování, a především jejich vztahy vůči subjektům údajů. Subjekty údajů musí být o podstatných prvcích způsobu spolupráce společných správců informovány. Subjekt údajů může vykonávat svá práva u každého ze společných správců i vůči každému z nich.
4. Správce musí se zpracovatelem uzavřít písemnou zpracovatelskou smlouvu. Zpracovatelská smlouva zejména stanoví:
   a) Předmět zpracování. Předmětem zpracování se míní vymezení okruhu osobních údajů, které mají být na základě zpracovatelské smlouvy zpracovávány. Předmět zpracování musí být vymezen dostatečně konkrétně tak, aby byly zřejmé alespoň
      i. konkrétní typy osobních údajů (např. jméno, příjmení, e-mail, kontaktní adresa),
      ii. kategorie osobních údajů a
      iii. kategorie subjektů údajů (např. zákazníci, zaměstnanci, dodavatelé).
   b) Dobu zpracování. Doba zpracování musí být stanovena jako přesný časový úsek nebo prostřednictvím kritérií, na základě kterých se přesný časový úsek určí (např. po dobu platnosti a účinnosti smlouvy apod.).
   c) Povahu a účel zpracování. Povaha zpracování uvedená ve zpracovatelské smlouvě musí být přiměřená účelu, pro který jsou osobní údaje zpracovávány správcem, a nesmí tomuto účelu odporovat. Účel zpracování uvedený ve zpracovatelské smlouvě nesmí být v rozporu s účelem zpracování na straně správce a nesmí ani tento účel svým rozsahem přesahovat. Smlouva by měla rovněž obsahovat upozornění, že v případě, kdy zpracovatel určí sám prostředky či účel zpracování, přestává být zpracovatelem a stává se správcem.
   d) Způsob řízení zpracovatele správcem. Osobní údaje mohou být zpracovatelem zpracovávány pouze na základě doložitelných pokynů správce. Zpracovatel informuje správce o zpracování, které je mimo pokyny správce povinen provést, jelikož mu tak stanoví právní řád.
   e) Mlčenlivost. Zpracovatel musí zajistit, aby se osoby zpracovávající svěřené osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.
   f) Bezpečnostní opatření. Zpracovatel musí být zavázán k přijetí dostatečných organizačních a technických opatření k zabezpečení zpracování osobních údajů dle a GDPR. Zpracovatel musí být zavázán k periodickým vnitřním auditům přijatých organizačních a-technických opatření na základě provedené analýzy rizik. Průběh vnitřních auditů a odůvodnění přijatých opatření musí být řádně zdokumentovány pro potřeby případného doložení plnění povinností.

g) Podmínky zapojení dalšího zpracovatele. Zpracovatel musí být zavázán k tomu, že bez předchozího písemného souhlasu správce nezapojí do zpracování žádného dalšího zpracovatele. Případný další zpracovatel musí být písemně zavázán ke zpracování osobních údajů způsobem souladným se zpracovatelskou smlouvou a dále k ochraně osobních údajů na alespoň takové úrovni, jaká je stanovena ve zpracovatelské smlouvě.

h) Poskytování součinnosti. Zpracovatel musí být zavázán k poskytování součinnosti v takovém rozsahu, aby správce mohl
   i. vyřizovat žádosti o výkon práv subjektů údajů způsobem a ve lhůtách dle těchto zásad a GDPR;
   ii. zajistit dostatečnou úroveň zabezpečení zpracování a ohlašovat bezpečnostní incidenty v souladu s vnitřními předpisy a čl. 32 až 36 GDPR;
   iii. doložit plnění povinností dle těchto Zásad a GDPR a
   iv. provádět audity u zpracovatele, a to buď sám, nebo prostřednictvím pověřeného auditora.

i) Opatření při ukončení zpracování. Zpracovatel musí být zavázán na základě rozhodnutí správce veškeré osobní údaje
   i. zlikvidovat (vymazat), vč. existujících kopií osobních údajů s výjimkou případů, kdy právní řád stanoví jinak, nebo
   ii. vrátit správci.

5. Smlouvy dle odst. 2. a 3. tohoto článku nemusí výslovně upravovat stanovené náležitosti v tom rozsahu, v jakém jsou již pro příslušné zpracovaní dostatečně upraveny právním řádem.
6. Správce do zpracování osobních údajů nezapojí externí subjekt, pokud by v důsledku tohoto zapojení nebyl správce schopen plnit své povinnosti dle těchto Zásad a GDPR.

XXXIII. Kontrola

1. Efektivitu a praktické fungování systému ochrany osobních údajů a bezpečnosti dat, jakož i plnění povinností Družstva dle GDPR a těchto Zásad v daném Družstvu přezkoumává kontrolní komise družstva, a to alespoň dvakrát ročně v pravidelných intervalech.
2. O výsledcích přezkumu písemnou zprávu bez zbytečného odkladu po skončení přezkumu, v níž bude zhodnocen zejména stav preventivních opatření, zranitelnosti a hrozby, závěry měření účinnosti přijatých opatření a doporučení pro zlepšení systému. Předseda kontrolní komise postoupí zprávu bez zbytečného odkladu vedení Družstva, které následně rozhodne o přijetí vhodných dodatečných opatření.