ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

UOOUX00EQ3CU

Čj. UOOU-00893/21-14
Praha 4. května 2021

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem 170 00 Praha 7 - Holešovice, Pplk. Sochora 727/27 (dále také „Úřad“)

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z čl. 58 odst. 1 písm. b) 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále také „nařízení (EU)2016/679“) a ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Kontrolující:

JUDr. Jiřina Rippelová - inspektorka Úřadu, průkaz inspektora č. 097, na základě pověření ke kontrole ze dne 23. února 2021, jako vedoucí kontrolní skupiny.

Mgr. Marta Lásiková - pověřená zaměstnankyně Úřadu, číslo průkazu: 196711323, na základě pověření ke kontrole ze dne 23. února 2021;

Kontrolovaná osoba:

XXXXX (dále jen „kontrolovaná osoba“)

Osoba jednající za kontrolovanou osobu:
XXXX

Místo provedení kontroly:

Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7

Předmět kontroly:

Předmětem kontroly je ověření postupů při zpracovávání osobních údajů a povinností vyplývajících z nařízení (EU) 2016/679 při využívání věrnostního programu a věrnostních karet, včetně rodinných karet zákazníky, a to především zaměřené na ověření zásad zpracování dle čl. 5 (zákonnost, minimalizace, omezení uložení, integrita a důvěrnost), zákonnosti zpracování podle čl. 6 (včetně případného profilování), podmínek udílení souhlasu dle čl. 7, výkonu práv subjektů údajů stanovených čl. 12-22 (zaměření na poskytování informací subjektům údajů a práva na výmaz), využití zpracovatelů podle čl. 28 či zabezpečení zpracování podle čl. 32 (zabezpečení databáze klientů) nařízení (EU) 2016/679.

První kontrolní úkon:
Kontrola byla zahájena doručením Oznámení o zahájení kontroly čj. UOOU-0893/21-3, ze dne 25. února 2021, které bylo kontrolované osobě doručeno dne 26. února 2021. Přílohou oznámení o zahájení kontroly bylo pověření ke kontrole čj. UOOU-00893/21-2 ze dne 23. února 2021.

Poslední kontrolní úkon: posledním kontrolním úkonem předcházejícím vyhotovení protokolu o kontrole byl *Úřední záznam - pořízení dokumentace ze dne 4. května 2021 Čj.* UOOU-00893/21-13*.*

1. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady (údaje, dokumenty a věci vztahující se k předmětu kontroly nebo k činnosti kontrolované osoby) a dokumenty, které byly pořízeny v průběhu kontroly, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti.

1. Kontrolní plán pro rok 2021 č.j. UOOU-00893/21-1, jeden list.
2. Oznámení o zahájení kontroly ze dne 25. února 2021. Doručeno 26. února 2021.Č.j. UOOU-OO893/21-3. 2 listy.
3. Sdělení kontrolované osoby k Oznámení o zahájení kontroly ze dne 25.02.2021 k čj.: UOOU-00893/21-3. Čj.: UOOU-00893/21-6.3 listy. 17 příloh.
   - 3.1. Zásady ochrany osobních údajů v souvislosti s používáním aplikace Xxxx, čtyři listy.
   - 3.2. Zásady ochrany osobních údajů společnosti Xxxx v souvislosti s Věrnostním programem „Xxxx Card“ dle čl. 13 Nařízení EU o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR), tři listy.
   - 3.3. Využívané programy při zpracování osobních/pseudoanonymizovaných dat v BI, jeden list.
   - 3.4. Zasílání partnerských kódů, tři listy.
   - 3.5. Záznamy v rámci registrace Xxxx Card a záznamy v rámci realizace kampaní přímého marketingu, osm listů.
   - 3.6. Individual Agreement on the provision of data protection-related services, šest listů.
   - 3.7. Eizelauftrag über die Erbringung datenschutzrevanter Dienstleistungen, šest listů.
   - 3.8. Vereinbarung zur Datenverarbeitung im Auftrag zwischen, patnáct listů.
   - 3.9. Smazání profilu zákazníka/uživatele (Zákaznický management/Revize), jeden list.
   - 3.10. Odpověď kontrolované osoby ze dne 25.11.2020, jeden list.

3.11. Odpověď kontrolované osoby ze dne 24.2.2021, dva listy.
3.12. Odpověď kontrolované osoby ze dne 12.3.2021, dva listy.
3.13. Vzor standardizované odpovědi kontrolované osoby, dva listy.
3.14. Standard-Datenschutz-Maßnahmen, 9 listů.
3.15. Standard Data Protection Measures, 8 listů.
3.16. Podmínky pro věrnostní program společnosti Xxxx, 4 listy.
3.17. Report žádostí, 1 list.

4. Odpověď na žádost o součinnost ze dne 24.03.2021 k č.j. UOOU-00893/21-7. Čj.: UOOU-00893/21-10.1 list. 4 přílohy.

4.1. Dílčí zakázka v oblasti poskytování služeb relevantních z pohledu ochrany osobních údajů - vzor, 6 listů.
4.2. Dílčí zakázka v oblasti poskytování služeb relevantních z pohledu ochrany osobních údajů - mezi kontrolovanou osobou a společností XXXX, 6 listů.
4.3. Dohoda o zpracování osobních údajů zpracovatelem, uzavřená mezi kontrolovanou osobou a Xxxx XXXX, Německo. 15 listů.
4.4. Standardní opatření ochrany osobních údajů (standardní technická a organizační opatření), 9 listů.

5. Odpověď na žádost o součinnost ze dne 30.04.2021 k č.j. UOOU-00893/21-7. Čj.: UOOU-00893/21-11.1 list. 2 přílohy.

5.1. Detailní pohled udělení souhlasu v aplikaci z webu - souhlasy Xxxx.
5.2. Souhlasy-interní pohled - AdobeCampaign.

6. Úřední záznam - pořízení dokumentace ze dne 4. května 2021, Čj. UOOU-00893/21-13*.*

6.1. Otisk webové stránky XXXX Podmínky použití: Věrnostní program „XXXXX“. 16 listů.

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v čase provedení kontroly a v rozsahu stanoveném v předmětu kontroly. Z výše uvedených podkladů pak byly pro kontrolní zjištění vyhodnoceny pouze ty části, v nichž jsou uvedeny relevantní informace ve vztahu k předmětu této kontroly.

2. Důvod kontroly:

Kontrola byla zahájena na základě Kontrolního plánu Úřadu pro rok 2021.
(podklad č.1)

3. Kontrolní zjištění:

Kontrolní zjištění č. 1:

Kontrolující se v rámci kontroly zaměřili a posuzovali zejména zpracování osobních údajů při využívání věrnostního programu a věrnostních karet, včetně rodinných karet zákazníky kontrolované osoby. Kontrolující předně posuzovali, zda informace, využívané v rámci věrnostního programu a věrnostních karet jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, a dále, zda jsou tyto údaje zpracovávány ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679.

K tomu kontrolující přikládají definici osobních údajů a též definici pojmu zpracování dle článku 4 odst. 1 nařízení (EU) 2016/679 a pojmu zpracování dle čl. 4 odst. 2 nařízení (EU) 2016/679:

> *„osobními údaji* (se rozumí) *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.“*
>
> *„zpracováním* (se rozumí) *jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů 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.“*

Kontrolou bylo zjištěno, že v rámci věrnostních karet Xxxx Card se zpracovávají následující údaje zákazníků/ uživatelů: pohlaví/oslovení, jméno a příjmení, titul (pokud je zákazníkem uveden), datum narození (k identifikačním účelům a pro účely ověření oprávnění k účasti na programu), heslo, které si zvolí zákazník (pro přihlášení na internetových stránkách věrnostního programu Xxxx Card a při vstupu do Xxxx Aplikace do sekce Xxxx Card), adresa (ulice, číslo domu, okres/obvod, PSČ, obec a země, a to pro účely identifikace, pro účely zasílání výher, je-li udělen souhlas, pak i pro účely zasílání reklamy a speciálních nabídek) a e-mailovou adresu a/nebo mobilní telefonní číslo (pro účely zasílání e-mailů/sms týkajících se stavu Věrnostního programu a pro účely autentifikace e-mailové adresy, resp. mobilního telefonního čísla prostřednictvím metody double opt-in a potvrzení registrace. Dále kontrolovaná osoba zpracovává údaje o prodejně Xxxx, ve které zákazník Věrnostního programu nakupuje a případně jeho nákupech, tj. informace týkající se produktů, které u kontrolované osoby zakoupil a v jakém množství a za jakou cenu, datum a čas nákupu a způsob platby za nákup (tj. hotovostní či bezhotovostní), (Podklad č. 3, 3.2).

V návaznosti na definici pojmu osobní údaj a definici zpracování osobních údajů, kontrolovaná osoba osobní údaje subjektů údajů zpracovává, a to s ohledem na předmět kontroly, minimálně v rozsahu jejich shromáždění, uložení, pozměňování, vyhledávání, uspořádání.

Kontrolující na základě výše uvedeného konstatují, že kontrolovaná osoba zpracovává ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679 osobní údaje ve smyslu čl. 4 odst. 1 nařízení (EU) 2016/679.

Kontrolní zjištění č. 2:

Kontrolující dále posuzovali, zda je kontrolovaná osoba v souvislosti s využíváním věrnostního programu a věrnostních karet, včetně rodinných karet zákazníky v postavení správce osobních údajů ve smyslu čl. 4 odst. 7 nařízení (EU) 2016/679, a hodnotili rovněž postavení a zapojení osoby zpracovatele, kterou je společnost Xxxx, ve smyslu čl. 4 odst. 8 nařízení (EU) 2016/679.

K tomu kontrolující přikládají definici pojmu správce osobních údajů a též definici pojmu zpracovatele:

> *„správcem* (se rozumí) *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení;“*
>
> *„zpracovatelem* (se rozumí) *fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce;“*

Kontrolou bylo zjištěno, že účelem zpracování osobních údajů v rámci účasti na Věrnostním programu kontrolované osoby je vytvoření vazby se zákazníky (subjekty údajů) formou sbírání digitálních věrnostních bodů, dále péče o uživatele (subjekty údajů) formou personalizovaných informací o nabídkách a akcích, neustálé zlepšování funkcionality a zajištění bezproblémového využívání věrnostní karty „Xxxx Card“. Z provedené kontroly je dále patrné, že kontrolovaná osoba shromažďuje osobní údaje subjektů údajů v rámci aplikace Xxxx. Byla to tedy kontrolovaná osoba, která určila účel a prostředky zpracování osobních údajů v rámci zpracování osobních údajů při využívání věrnostního programu a věrnostních karet (podklad č. 3,3.1 a 3.2.).

Kontrolou bylo dále zjištěno, že zpracovatelem osobních údajů je společnost Xxxx, která poskytuje kontrolované osobě služby v oblasti softwaru pro správu pojištění, online oznamovací systém (BKMS) vč. referentské podpory, provádění revizních opatření, péči o zákazníky, reklamu, správu vozového parku, personální management (SAP HCM)-omezený přístup, personální management (SAPH HCM) - dočasný neomezený přístup, provádění oborových analýz personálních struktur, licenční management, cestovní management/expense, Jabber, management nákupních nástrojů, mystery experience checks (podklad č. 4.3).

Kontrolující s ohledem na výše uvedené konstatují, že kontrolovaná osoba je v rámci využívání věrnostních karet „Xxxx Card“ v postavení správce podle čl. 4 odst. 7 nařízení (EU) 2016/679, neboť určila účel a prostředky předmětného zpracování osobních údajů. Společnost Xxxx Xxxx se nachází v rámci předmětné činnosti v postavení zpracovatele ve

smyslu čl. 4 odst. 8 nařízení (EU) 2016/679, neboť pro správce, kontrolovanou osobu, osobní údaje zpracovává v rozsahu Dohody o zpracování osobních údajů zpracovatelem.

Kontrolní zjištění č. 3:

V návaznosti na kontrolní zjištění č. 2 kontrolující hodnotili, zda byla mezi kontrolovanou osobou, v postavení správce osobních údajů a společností Xxxx Xxxx, v postavení zpracovatele, uzavřena smlouva o zpracování osobních údajů či jiný právní akt, jak je pro případ zpracování osobních údajů zpracovatelem stanoveno čl. 28 odst. 3 nařízení (EU) 2016/679.

K tomu kontrolující přikládají znění ustanovení čl. 28 odst. 3 nařízení (EU) 2016/679:

> *„Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, 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:*
>
> *a) 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, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;*
>
> *b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti:*
>
> *c) přijme všechna opatření požadovaná podle článku 32;*
>
> *d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;*
>
> *e) 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 stanovených v kapitole III;*
>
> *f) je správci nápomocen při zjišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;*
>
> *g) 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 Unie nebo členského státu nepožaduje uložení daných osobních údajů;*
>
> *h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje.*
>
> *Pokud jde o první pododstavec písm. h) informuje zpracovatel neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů.“*

Provedenou kontrolou bylo zjištěno (podklad č. 4.3), že kontrolovaná osoba/objednatel uzavřela se společností Xxxx Xxxx, Dohodu o zpracování osobních údajů, jejímž předmětem je pověření poskytováním služeb v oblasti softwaru pro správu pojištění, online oznamovací systém (BKMS) vč. referentské podpory, provádění revizních opatření, péči o zákazníky, reklamu, správu vozového parku, personální management (SAP HCM)-omezený přístup, personální management (SAPH HCM) - dočasný neomezený přístup, provádění oborových analýz personálních struktur, licenční management, cestovní management/expense, Jabber, management nákupních nástrojů, mystery experience checks. Předmětem je rovněž poskytování a péče o postupy při zpracování osobních údajů, služby zahrnující vzdálený přístup, multimediální a telekomunikační služby. Přesný seznam služeb, jejichž poskytováním byl pověřen Dodavatel, je obsažen v Příloze 1 výše uvedené Dohody o zpracování osobních údajů.
Příslušná ustanovení smlouvy zavazují zpracovatele (v roli dodavatele) ke zpracování osobních údajů pro účely shora uvedené. Zpracovatel/Dodavatel smí zpracovávat osobní údaje na základě doložených pokynů kontrolované osoby/objednatele. Zpracovatel/Dodavatel se zavazuje, že bude osobní údaje řádně zpracovávat, a že přijme technická a organizační opatření. K tomuto patří zejména bezpečnostní koncept, který specifikuje, na základě jakých technických a organizačních mechanismů bude zajištěna důvěrnost, integrita a dostupnost osobních údajů zpracovávaných v rámci poskytování služeb.

Kontrolující na základě uvedeného konstatují, že zpracování osobních údajů zpracovatelem se řídí smlouvou naplňující požadavky čl. 28 odst. 3 nařízení (EU) 2016/679.

Kontrolní zjištění č. 4:

Kontrolující dále posuzovali zákonnost zpracování osobních údajů, zda je zpracování osobních údajů, jenž je předmětem této kontroly, zákonné ve smyslu čl. 6 odst. 1, dle kterých musí správce osobních údajů pro dané zpracování vždy disponovat legitimním právním titulem, tedy zpracovávat osobní údaje pouze v případech taxativně vyjmenovaných v čl. 6 odst. 1 písm. a) až f) nařízení (EU) 2016/679.

K tomu kontrolující přikládají znění ustanovení čl. 6 odst. 1 písm. a) až f) nařízení (EU) 2016/679:

Článek 6 (právní titul)

„Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;

b) 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;

c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;

d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;

e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;

f) 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.

První pododstavec písm. f) se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů.“

Kontrolou bylo zjištěno (podklad č. 3 a 3.2), že právním titulem pro zpracování osobních údajů v případě základního členství ve věrnostním programu Xxxx Card je čl. 6 odst. 1 b) nařízení EU 2016/679, tedy zpracování nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů. Dalším právním titulem pro kontrolovanou osobu je zpracování 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, tedy čl. 6 odst. 1 f) nařízení EU 2016/679, (např. služba K Scan, sada nástrojů Facebook SDK, analytický nástroj Google Firebase). V případě zpracování osobních údajů v souvislosti se zasíláním reklamních sdělení je právním titulem zpracování osobních údajů souhlas subjektu údajů, tedy čl. 6 odst. 1 a) nařízení EU 2016/679. V souvislosti s využíváním Xxxx se jedná o takzvaný systémový souhlas, kdy zákazník v aplikaci nebo na webu po seznámení se Zásadami ochrany osobních údajů a vyplnění kontaktních údajů bere na vědomí dané zpracování a souhlas uděluje pomocí prokliku s přesnou textací: „Potvrzuji, že souhlasím se Zásadami ochrany osobních údajů“. Současně má možnost nastavit si, zda si přeje dostávat informace o nabídkách a výhodách Xxxx, případně zvolí způsob této komunikace (sms, email, pošta). Kontrolovaná osoba doložila detailní pohled udělení souhlasu v aplikaci i z webových stránek (podklad č. 5, 5.1 a 5.2).

Kontrolující na základě výše uvedeného konstatují, že kontrolovaná osoba postupuje při zpracování osobních údajů u využívání věrnostního programu a věrnostních karet v souladu s čl. 6 odst. 1 nařízení (EU) 2016/679, neboť osobní údaje zpracovává pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, tedy dle čl. 6 odst.1 písm. b) nařízení (EU) 2016/679 a dále na základě právního titulu uvedeném v čl. 6 odst. 1 písm. a) a f) nařízení (EU) 2016/679.

Kontrolní zjištění č. 5:

Kontrolující taktéž posuzovali, jakým způsobem dochází k naplňování zásady ve smyslu čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, zejména ve vztahu k transparentnosti

zpracování, a dále plnění povinností, které v souvislosti se zpracováním osobních údajů vyplývají kontrolované osobě ze znění čl. 12 a 13 nařízení (EU) 2016/679.

V této souvislosti kontrolující citují čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679:

„Článek 5 odst. 1 Osobní údaje musí být

a) *ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);*
b) *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 podle čl. 89 odst. 1 nepovažuje za neslučitelné s původními účely („účelové omezení“);*
c) *přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („minimalizace údajů“);*
d) *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“);*
e) *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 podle čl. 89 odst. 1, a to za předpokladu provedení příslušných technických a organizačních opatření požadovaných tímto nařízením s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);*
f) *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“);“*

K tomu kontrolující citují čl. 12 nařízení (EU) 2016/679:
„Článek 12 Transparentní informace, sdělení a postupy pro výkon práv subjektu údajů

1. *Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článcích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.*

2. *Správce usnadňuje výkon práv subjektu údajů podle článků 15 až 22. V případech uvedených v čl. 11 odst. 2 správce neodmítne vyhovět žádosti subjektu údajů za účelem výkonu jeho práv podle článků 15 až 22, ledaže doloží, že nemůže zjistit totožnost subjektu údajů.*

3. *Správce poskytne subjektu údajů na žádost podle článků 15 až 22 informace o přijatých opatřeních, a to bez zbytečného odkladu a v každém případě do jednoho měsíce od obdržení žádosti. Tuto lhůtu je možné v případě potřeby a s ohledem na složitost a počet žádostí prodloužit o další dva měsíce. Správce informuje subjekt údajů o jakémkoliv takovém prodloužení do jednoho měsíce od obdržení žádosti spolu s důvody pro tento odklad. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, je-li to možné, pokud subjekt údajů nepožádá o jiný způsob.*

4. *Pokud správce nepřijme opatření, o něž subjekt údajů požádal, informuje bezodkladně a nejpozději do jednoho měsíce od přijetí žádosti subjekt údajů o důvodech nepřijetí opatření a o možnosti podat stížnost u dozorového úřadu a žádat o soudní ochranu.*

5. *Informace podle článků 13 a 14 a veškerá sdělení a veškeré úkony podle článků 15 až 22 a 34 se poskytují a činí bezplatně. Jsou-li žádosti podané subjektem údajů zjevně nedůvodné nebo nepřiměřené, zejména protože se opakují, může správce buď:*
   a) *uložit přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo sdělení nebo s učiněním požadovaných úkonů; nebo*
   b) *odmítnout žádosti vyhovět.*

   Zjevnou nedůvodnost nebo nepřiměřenost žádosti dokládá správce.

6. *Aniž je dotčen článek 11, pokud má správce důvodné pochybnosti o totožnosti fyzické osoby, která podává žádost podle článků 15 až 21, může požádat o poskytnutí dodatečných informací nezbytných k potvrzení totožnosti subjektu údajů.*

7. *Informace, které mají být subjektům údajů poskytnuty podle článků 13 a 14, mohou být doplněny standardizovanými ikonami s cílem poskytnout snadno viditelným, srozumitelným a jasným způsobem přehled o zamýšleném zpracování. Pokud jsou ikony prezentovány v elektronické formě, jsou strojově čitelné.*

8. *Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 92 za účelem určení informací, které mají být sděleny pomocí ikon, a postupů pro poskytování standardizovaných ikon.“*

Dále kontrolující citují článek 13 nařízení (EU) 2016/679:
„Článek 13 Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů.

1. *Pokud se osobní údaje týkající se subjektu údajů získávají od subjektu údajů, poskytne správce v okamžiku získání osobních údajů subjektu údajů tyto informace:*
   a) *totožnost a kontaktní údaje správce a jeho případného zástupce;*
   b) *případně kontaktní údaje případného pověřence pro ochranu osobních údajů;*
   c) *účely zpracování, pro které jsou osobní údaje určeny, a právní základ pro zpracování;*

d) oprávněné zájmy správce nebo třetí strany v případě, že je zpracování založeno na čl. 6 odst. 1 písm. f);
e) případné příjemce nebo kategorie příjemců osobních údajů;
f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně nebo, v případech předání uvedených v článcích 46 nebo 47 nebo čl. 49 odst. 1 druhém pododstavci, odkaz na vhodné záruky a prostředky k získání kopie těchto údajů nebo informace o tom, kde byly tyto údaje zpřístupněny.

2. Vedle informací uvedených v odstavci 1 poskytne správce subjektu údajů v okamžiku získání osobních údajů tyto další informace, jsou-li nezbytné pro zajištění spravedlivého a transparentního zpracování:
a) doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;
b) existence 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;
c) pokud je zpracování založeno na čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a), existence práva odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;
d) existence práva podat stížnost u dozorového úřadu;
e) 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;
f) skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, uvedenému v čl. 22 odst. 1 a 4, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.

3. Pokud správce hodlá osobní údaje dále zpracovávat pro jiný účel, než je účel, pro který byly shromážděny, poskytne subjektu údajů ještě před uvedeným dalším zpracováním informace o tomto jiném účelu a příslušné další informace uvedené v odstavci 2.

4. Odstavce 1, 2 a 3 se nepoužijí, pokud subjekt údajů již uvedené informace má, a do té míry, v níž je má.“

Kontrolující konstatují, že cílem kontrolované osoby je zajistit dodržování zásad zákonnosti a korektnosti zpracování osobních údajů a splnění informační povinnosti vůči příslušnému subjektu údajů. Informační povinnost je kontrolovanou osobu plněna v několika rovinách. Každý subjekt údajů (zákazník/uživatel Xxxx Card) kontrolované osoby je se svými právy seznámen vždy před registrací do Věrnostního programu a případným souhlasem s podmínkami. Tyto podmínky, včetně informací o právech zákazníků/uživatelů a jejich uplatnění jsou následně také k dispozici na internetových stránkách kontrolované osoby XXXX. Stejně tak mají zákazníci/uživatelé kontrolované osoby přístup v rámci mobilní aplikace (podklad č. 3 a 3.2),

Informace obsahuje:
1. Správce osobních údajů ve smyslu čl. 4 č. 7 GDPR
2. Kontaktní formulář / e-mailový kontakt / telefonní hovory
3. Zákaznický profil Xxxx a nákupní lístek
4. Přihlášení přes sociální sítě
5. Hry o ceny
6. Souhlas se zasíláním reklamního newsletteru e-mailem
7. Souhlas se zasíláním reklamních newsletterů prostřednictvím aplikace WhatsApp
8. Automatické vyhledání prodejny
9. Použití textových souborů cookies
9.1 Webtracking prostřednictvím aplikace Adobe Analytics
9.2 Google Conversion Tracking
9.3 Reklamní síť Google Display
9.4 Technologie Facebook Conversion Tracking
9.5 Retargeting a měření úspěšnosti reklamy Double Click
9.6 Retargeting a měření úspěšnosti reklamy Sklik
9.7 Doba trvání uložení / kritéria pro stanovení doby trvání uložení u cookies
9.8 Shrnutí všech možností odmítnutí
10. Integrované zvukové soubory Soundcloud
11. Integrovaná videa Youtube
12. Funkce a obsah Google Maps
13. Šifrování
14. Vaše příslušná práva
15. Kontakt pro ochranu osobních údajů

Při zpracování osobních údajů jsou předem definovány příslušné účely zpracování, které jsou písemně zaznamenány v příslušném formuláři týkajícím se záznamů o činnostech zpracování. Je-li to možné a lze-li toho dosáhnout s využitím přiměřených nákladů jsou osobní údaje v systémech pseudonymizovány, stejně tak aktualizovány. Po uplynutí regulérních lhůt výmazu jsou údaje vymazány.
Kontrolou bylo zjištěno, že kontrolovaná osoba od spuštění věrnostního programu Xxxx Card do dne zahájení kontroly obdržela čtyři žádosti o informace o zpracování osobních údajů dle čl. 15 nařízení (EU) 2016/679 a informace dle čl. 12 odst. 3 poskytla, což doložila (podklad č.3,3.10,3.11,3.12,3.13, 4.1.).

Kontrolující na základě výše uvedeného shrnují, že kontrolovaná osoba, jako správce osobních údajů přijala vhodná opatření, aby poskytla subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v článku 12 a 13 a učinila veškerá sdělení podle článku 15 nařízení (EU) 2016/679. Povinnosti stanovené čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679 a čl. 12 a 13 nařízení (EU) 2016/679 tak kontrolovaná osoba neporušila.

Kontrolní zjištění č. 6:
Kontrola automatizovaného individuálního rozhodování, včetně profilování. Kontrola se taktéž zaměřila na čl. 22 nařízení (EU)2016/679.

V této souvislosti kontrolující citují čl. 22 odst. 1 až 4 nařízení (EU) 2016/679:

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. Odstavec 1 se nepoužije, pokud je rozhodnutí:
a) nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů;
b) povoleno právem Unie 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
c) založeno na výslovném souhlasu subjektu údajů.
3. V případech uvedených v odst. 2 písm. a) a c) provede správce údajů vhodná opatření na ochranu práv a svobod a oprávněných zájmů subjektu údajů, alespoň práva na lidský zásah ze strany správce, práva vyjádřit svůj názor a práva napadnout rozhodnutí.
4. Rozhodnutí uvedená v odstavci 2 se neopírají o zvláštní kategorie osobních údajů uvedené v čl. 9 odst. 1, pokud se neuplatní čl. 9 odst. 2 písm. a) nebo g) a nejsou zavedena vhodná opatření pro zajištění práv a svobod a oprávněných zájmů subjektu údajů.

Provedenou kontrolou bylo zjištěno, že v rámci Věrnostního programu „Xxxx Card" dochází k automatizovanému zpracování osobních údajů (prostřednictvím automatizovaných prostředků, tj. prostředků výpočetní techniky). Subjekt údajů však není předmětem žádného rozhodnutí založeném výhradně na automatizovaném zpracování, včetně profilování.
Kontrolovaná osoba informuje subjekty údajů prostřednictvím *Zásad ochrany osobních údajů společnosti Xxxx v souvislosti s Věrnostním programem „Xxxx Card" dle čl. 13 nařízení (EU) 2016/679.*
V *Podmínkách pro využívání personalizovaných nabídek pro účastníky věrnostního programu „Xxxx Card"* je stanoveno v bodě 2. *Podmínky účasti,* že *aby mohl uživatel využívat personalizované reklamní nabídky, musí mít založený on- line účet v Aplikaci Xxxx pro Xxxx Card a musí vyslovit souhlas s podmínkami užívání a zásadami ochrany osobních údajů, a nebo musí být držitelem registrované Xxxx Card a vyslovit souhlas s podmínkami užívání a zasíláním personalizovaných nabídek prostřednictvím jím zvoleného komunikačního kanálu, a to v uživatelském rozhraní na webu xxxx.cz anebo na terminálu umístěném v obchodních domech Xxxx.*
Kontrolovaná osoba sdělila, že *profilování a automatizované zpracování s cílem poskytovat určitým zákaznickým segmentům specifické nabídky je zatím ve fázi vývoje, a že v České republice není ke komunikaci se zákazníkem nijak využíváno. Využívají se především agregovaná data k analýze větších celků (chování zákazníků určitých filiálek/v určitých dnech nebo hodinách, podle věkového rozsahu, místa bydliště apd.). Kontrolovaná osoba však cíleně nevyhledává ani nezpracovává osobní údaje na úrovni zákazníků* (podklad č.3.2,3.3,3.4,6.1).

Kontrolovaná osoba postupuje v souladu s článkem 22 nařízení (EU) 2016/679.
Kontrolní zjištění č. 7

Předmětem kontroly byla rovněž kontrola plnění povinností stanovené v čl. 30 nařízení (EU) 2016/679 - vést záznamy o činnostech zpracování.

V této souvislosti kontrolující citují čl. 30 odst. 1 až 4 nařízení (EU) 2016/679:

1. *„Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá. Tyto záznamy obsahují všechny tyto 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, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;
   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 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 uvedených v čl. 32 odst. 1.

2. *Každý zpracovatel a jeho případný zástupce vede záznamy o všech kategoriích činností zpracování prováděných pro správce, jež obsahují: a) jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů; b) kategorie zpracování prováděného pro každého ze správců; c) 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 doložení vhodných záruk; d) je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.*

3. *Záznamy podle odstavců 1 a 2 se vyhotovují písemně, v to počítaje i elektronickou formu.*

4. *Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu.“*

Kontrolou bylo zjištěno, že kontrolovaná osoba má zpracované záznamy o činnostech zpracování, které obsahují kontaktní údaje správce, právní základ a účely zpracování osobních údajů, popis jednotlivých kategorií subjektů údajů a kategorií osobních údajů, kategorii příjemců, kterým budou osobní údaje zpřístupněny, popis technických a organizačních bezpečnostních opatření (podklad 3.5.).

Kontrolovaná osoba má zpracované a vede Záznamy o činnostech zpracování, které obsahují veškeré informace, které stanoví čl. 30 nařízení (EU) 2016/679 a postupovala tak v souladu s tímto článkem nařízení.

Kontrolní zjištění č. 8

Kontrola zabezpečení osobních údajů. Kontrola se v neposlední řadě zaměřila na plnění povinností stanovených v čl. 32 nařízení (EU)2016/679.

V této souvislosti kontrolující citují čl. 32 body 1 a 2 nařízení (EU) 2016/679; Zabezpečení zpracování:

1. *„S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající riziku, případně včetně:*
   a) *Pseudonymizace a šifrování osobních údajů:*
   b) *Schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování:*
   c) *Schopnost obnovit dostupnost osobních údajů a přístup k nim včas, případě fyzických či technických incidentů.*
   d) *Procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.*

2. *Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.“*

Kontrolou bylo zjištěno, že kontrolovaná osoba má zpracovaný dokument „Standardní opatření v oblasti ochrany osobních údajů (standardní technická a organizační opatření)“. Je-li to možné a přiměřené s ohledem na sledovaný účel zpracování, jsou osobní údaje zpracovávány pseudonymně. Příslušná opatření jsou dokumentována ohledně každého procesu, IT systému nebo jiného zpracování. Účinnost metod a postupů používaných k šifrování a souvisejících procesů týkajících se správy elektronických klíčů a certifikátů je pravidelně ověřována/testována a v případě potřeby upravována. V závislosti na míře potřeby ochrany se v případě databází použije transparentní šifrování dat (šifrování TDE). Procesy a postupy zabezpečení informací jsou definovány jako součást systému řízení bezpečnosti informací (ISMS) na základě normy ISO/IEC 27001 a násl. uvedené procesy a postupy podléhají pravidelné kontrole a v případě potřeby jsou pravidelně aktualizovány. Zaměstnanci kontrolované osoby jsou zavázáni dodržovat důvěrnost osobních údajů a jsou přiměřeným způsobem např. formou školení a informačních kampaní informování o požadavcích a povinnostech týkajících se ochrany osobních údajů a zabezpečení informací. Při zpracování osobních údajů zpracovatelem na základě pověření ze strany správce je řádně vypracovaná související smluvní dokumentace. V rámci kontrolního zjištění č. 3 bylo zjištěno, že kontrolovaná osoba má uzavřenou Dohodu o zpracování osobních údajů, se společností Xxxx Xxxx, (podklad č. 4.3 a 4.4).

Kontrolovaná osoba tak naplnila všechny povinnosti, které jí ukládá č. 32 odst. 1 a 2 nařízení (EU) 2016/679 a jednala tak v souladu s tímto článkem nařízení.

I. Poučení o opravném prostředku:

Proti kontrolním zjištěním uvedeným v protokolu o kontrole může kontrolovaná osoba podat Úřadu pro ochranu osobních údajů ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky.

Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Podpisová doložka:

otisk
úředního
razítka

JUDr. Jiřina Rippelová	inspektorka	
……	……..	……..
titul jméno příjmení	funkce	podpis

Mgr. Marta Lásiková	pověřená zaměstnankyně	
……..	……..	……..
titul jméno a příjmení	funkce	podpis