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

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7 (dále jen „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 jen „nařízení (EU) 2016/679“) ve spojení s § 50 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Kontrolující:

Mgr. et Mgr. Božena Čajková (vedoucí kontrolní skupiny)
jako inspektorka Úřadu, č. průkazu: XXXX, na základě pověření ke kontrole ze dne 17. února 2021,
jako pověřená zaměstnankyně Úřadu, na základě pověření ke kontrole ze dne 3. června 2021;

Bc. Hana Imiolková – pověřená zaměstnankyně Úřadu, č. průkazu: XXXXXX, na základě pověření ke kontrole ze dne 17. února 2021;

Mgr. Zuzana Jeřábková – pověřená zaměstnankyně Úřadu, č. průkazu: XXXXXX, na základě pověření ke kontrole ze dne 17. února 2021.

Kontrolovaná osoba:

XXXXXXXXXXX (dále jen „kontrolovaná osoba“nebo „XXXXXX“)

Předmět kontroly:

Předmětem kontroly je dodržování povinností stanovených nařízením (EU) 2016/679 a zákonem č. 110/2019 Sb. v souvislosti se zpracováním osobních údajů subjektů údajů v rámci věrnostního programu obchodního řetězce.

První kontrolní úkon:

Oznámení o zahájení kontroly čj. UOOU-00807/21-3, ze dne 19. února 2021.

Poslední kontrolní úkon:

Úřední záznam o pořízení dokumentace ze dne 1. července 2021, čj. UOOU-00807/21-29.

I. Přehled podkladů:

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti:

1. Kontrolní plán Úřadu pro rok 2021;
2. Oznámení o zahájení kontroly ze dne 19. února 2021, čj. UOOU-00807/21-3, počet stran 3;
   2.1. příloha – pověření ke kontrole, počet stran 1;
3. Vyjádření kontrolované osoby ze dne 30. března 2021, čj. UOOU-00807/21-6, počet stran 7;
   3.1. příloha – P1_Přehled evidencí, počet stran 4;
   3.2. příloha – P2_XXXXXXX_seznam_zpracovatelu_ou, počet stran 1;
   3.3. příloha – XXXXXXXXX_Dodatek_o_zpracovani_a_ochrane_OU, počet stran 8;
   3.4. příloha – _Smlouva_o_zajistovani_reklamniho_prostoru, počet stran 3;
   3.5. příloha – XXXXXX_Ramcova_smlouva_o_poskytovani_suzeb_OU, počet stran 9;
   3.6. příloha – XXXXX_Dodatek_o_zpracovani_a_ochrane_OU_k_Smlouvě_o_dílo, počet stran 7;
   3.7. příloha – XXXX_Servisni_smlouva_zpracovani_a_ochrana_OU, počet stran 18;
   3.8. příloha – XXXXX_Smlouva_o_dilo, počet stran 23;
4. Vyjádření kontrolované osoby ze dne 30. března 2021 (XXXXX_Smlouva_o_pronajmu_vyhrazeneho_tymu_zpracovani_a_ochrana_OU.pdf), čj. UOOU-00807/21-7, počet stran 13;
   4.1. příloha – XXXXX_Dodatek_o_zpracovani_a_ochrane_OU, počet stran 10;
   4.2. příloha – XXXXXX_Smlouva_o_zrizeni_sluzby_web_standard, počet stran 5;
   4.3. příloha – XXXXXX_Dodatek_o_zpracovani_OU_k_Smlouve_o_udrzbe, počet stran 7;
   4.4. příloha – XXXXXX_Smlouva_o_poskytovani_servisnich_sluzeb_OU, počet stran 20;
5. Vyjádření kontrolované osoby ze dne 30. března 2021 (XXXXXXX_Smlouva_o_udrzbe_a_servisni_podpor), čj. UOOU-00807/21-8, počet stran 10;

5.1. příloha – XXXXX_Dodatek_o_zpracovani_a_ochrane_OU, počet stran 6;
5.2. příloha – XXXXX_smlouva_o_poskytovani_sluzeb, počet stran 10;
5.3. příloha – P3_XXXXXXX_Zaznamy_zpracovani, počet stran 15;
5.4. příloha – P4_XXXXX_papirovy_registracni_formular, počet stran 2;

6. Vyjádření kontrolované osoby ze dne 30. března 2021 (P5_XXXXX_informace_o_ochrane_ou_formular), čj. UOOU-00807/21-9, počet stran 2;
6.1. příloha – P6_Přehled_žádostí, počet stran 3;
6.2. příloha – P7_Technicko_organizační_opatření_1_4_XXXXX, počet stran 12;
6.3. příloha – P8_IT_Užívání_IT_systémů, počet stran 10;
6.4. příloha – P9_Objektová_Směrnice_pro_výkon_strážní_služby_XXX, počet stran 15;
6.5. příloha – P10_Pravidla_chovani_v_datových_centrech, počet stran 5;
6.6. příloha – P11_Směrnice_zálohování, počet stran 2;
6.7. příloha – P12_Autentizace_zakaznika_Uzivatelska_dokumentace_01_02, počet stran 18;
6.8. příloha – P13_Autentizace_zakaznika_Technicka_dokumentace_01_00, počet stran 20;
6.9. příloha – P14_IS_3_2_3_Access_management_policy_CZ, počet stran 10;
6.10. příloha – P15_IncidentManagement_CZ, počet stran 35;

7. Úřední záznam o pořízení dokumentace ze dne 19. dubna 2021, čj. UOOU-00807/21-11, počet stran 1;
7.1. příloha – výtisk internetové stránky Registrace do programu XXXXXX. URL: [https://www.XXXXXXXXXX/prihlaseni/registrace]. počet stran 1;
7.2. příloha – výtisk internetové stránky První přihlášení s kartou. URL: [https://www.XXXXXXXX.cz/prihlaseni/prvni-prihlaseni?]. počet stran 1;
7.3. příloha – snímek obrazovky Registrace krok 1 – Pro koho bude karta? URL: [https://XXXXXX.cz/prohlaseni/registrace/krok1];
7.4. příloha – výtisk internetové stránky Registrace krok 2 – Kam chcete zasílat slevové kupóny? URL: [https://XXXXXX.cz/prohlaseni/registrace/krok2]. počet stran 1;
7.5. příloha – snímek obrazovky Registrace krok 3 – Registrace do Mimi klubu URL: [https://XXXXXX.cz/prohlaseni/registrace/dite];
7.6. příloha – výtisk internetové stránky Registrace krok 4 – Zkontrolujte si Vaše údaje URL: [https://XXXXXXX.cz/prohlaseni/registrace/krok4]. počet stran 1;
7.7. příloha – snímek obrazovky Registrace krok 4 – závěrečná ujednání 1 [https://XXXXXXX.cz/prohlaseni/registrace/krok4];
7.8. příloha – snímek obrazovky Registrace krok 4 – závěrečná ujednání 2 [https://XXXXXXX.cz/prohlaseni/registrace/krok4].

8. Protokol o z ústního jednání ze dne 26. dubna 2021, Čj. UOOU-00807/21-12, počet stran 3;
9. Vyjádření kontrolované osoby ze dne 3. května 2021, čj. UOOU-00807/21-13, počet stran 2;
9.1. příloha – Přehled žádostí (P1_Přehled_žádostí), počet stran 3;
9.2. příloha – Zpracování osobních údajů zákazníka, který uskutečňuje online nákup (P2_online_nakup), počet stran 2;
10. Vyjádření kontrolované osoby ze dne 10. května 2021, čj. UOOU-00807/21-15, počet stran 4;
10.1. příloha – Přehled osobních údajů zpracovávaných ve VP dle jednotlivých databází u vybraných zákazníků, počet stran 3;

10.2. příloha – Informace o osobních údajích S. A., počet stran 1;
10.3. příloha – Zaznamenaná historie bonusů S. A., počet stran 1;
10.4. příloha – Zaznamenaná historie komunikace a změny provedené v zákaznickém účtu S. A., počet stran 1;
10.5. příloha – Zaznamenaná historie kupónů S. A., počet stran 1;
10.6. příloha – Registrační formulář S. A., počet stran 1;
10.7. příloha – Informace o osobních údajích K. J., počet stran 1;
10.8. příloha – Zaznamenaná historie bonusů K. J., počet stran 1;
10.9. příloha – Zaznamenaná historie komunikace a změny provedené v zákaznickém účtu K. J., počet stran 1;
10.10. příloha – Zaznamenaná historie kupónů K. J., počet stran 1;
10.11. příloha – Registrační formulář K. J., počet stran 1;
10.12. příloha – Informace o osobních údajích J. S., počet stran 1;
10.13. příloha – Zaznamenaná historie bonusů J. S., počet stran 1;
10.14. příloha – Zaznamenaná historie komunikace a změny provedené v zákaznickém účtu J. S., počet stran 1;
10.15. příloha – Zaznamenaná historie kupónů J. S., počet stran 1;
10.16. příloha – Registrační formulář J. S., počet stran 1;
10.17. příloha – Informace o osobních údajích M. Č., počet stran 1;
10.18. příloha – Zaznamenaná historie bonusů M. Č., počet stran 1;
10.19. příloha – Zaznamenaná historie komunikace a změny provedené v zákaznickém účtu M. Č., počet stran 3;
10.20. příloha – Zaznamenaná historie kupónů M. Č., počet stran 1;
10.21. příloha – Registrační formulář M. Č., počet stran 1;
10.22. příloha – Informace o osobních údajích E. R., počet stran 1;
10.23. příloha – Zaznamenaná historie bonusů E. R., počet stran 1;
10.24. příloha – Zaznamenaná historie komunikace a změny provedené v zákaznickém účtu E. R., počet stran 1;
10.25. příloha – Zaznamenaná historie kupónů E. R., počet stran 1;
10.26. příloha – Registrační formulář E. R., počet stran 1;
10.27. příloha – Směrnice Zpracování a ochrana osobních údajů (P2_a_G_Zpracování_a_ochrana_osobních_údajů), počet stran 8;
10.28. příloha – Pokyny pro zaměstnance Pokyny ke zpracování osobních údajů pro informační a reklamační pracovníky (P2_b_G_Pokyny_info_a_reklamace), počet stran 4;
10.29. příloha – Pokyny pro zaměstnance Pokyny ke zpracování osobních údajů pro zaměstnance oddělení marketing a multichannel (P2_c_G_Pokyny_marketing_a_multichannel), počet stran 3;
10.30. příloha – Přehled přístupů XXXXX správců k databázím pro den 14. dubna 2021 (P3_Přehled_záznamů_přístupů_zaměstnanců), počet stran 35;
10.31. příloha – Popis pracovní pozice A. H., počet stran 3;
10.32. příloha – Popis pracovní pozice H. R., počet stran 3;
10.33. příloha – Popis pracovní pozice H. M., počet stran 3;
11. Popis pracovní pozice I. R., čj. UOOU-00807/21-14, počet stran 3;
11.1. příloha – Popis pracovní pozice I. S., počet stran 3;
11.2. příloha – Popis pracovní pozice J. V., počet stran 3;
11.3. příloha – Popis pracovní pozice J. N., počet stran 3;
11.4. příloha – Popis pracovní pozice J. Š., počet stran 3;

11.5. příloha – Popis pracovní pozice J. V., počet stran 3;
11.6. příloha – Popis pracovní pozice K. M., počet stran 3;
12. Popis pracovní pozice I. R., čj. UOOU-00807/21-16, počet stran 3;
12.1. příloha – Popis pracovní pozice L. K., počet stran 5;
12.2. příloha – Popis pracovní pozice L. P, počet stran 3;
12.3. příloha – Popis pracovní pozice L. K., počet stran 3;
12.4. příloha – Popis pracovní pozice M. Č., počet stran 3;
13. Popis pracovní pozice M. D., čj. UOOU-00807/21-17, počet stran 3;
13.1. příloha – Popis pracovní pozice M. P., počet stran 3;
13.2. příloha – Popis pracovní pozice M. K., počet stran 3;
13.3. příloha – Popis pracovní pozice M. Z., počet stran 3;
13.4. příloha – Popis pracovní pozice O. Š., počet stran 3;
13.5. příloha – Popis pracovní pozice R. B., počet stran 3;
13.6. příloha – Popis pracovní pozice R. Š., počet stran 3;
13.7. příloha – Popis pracovní pozice R. J., počet stran 3;
14. Popis pracovní pozice R. R., čj. UOOU-00807/21-18, počet stran 3;
14.1. příloha – Popis pracovní pozice T. S., počet stran 3;
14.2. příloha – Popis pracovní pozice V. D., počet stran 3;
14.3. příloha – Popis pracovní pozice Z. P, počet stran 3;
14.4. příloha – Popis pracovní pozice Z. F., počet stran 3;
14.5. příloha – Popis pracovní pozice Z. R., počet stran 3;
14.6. příloha – Vzor pracovní smlouvy, počet stran 4;
15. Pověření ke kontrole ze dne 3. června 2021, čj. UOOU-00807/21-20, počet stran 1;
16. Vyjádření kontrolované osoby ze dne 7. června 2021, čj. UOOU-00807/21-21, počet stran 2;
16.1. příloha – 2019_01_16_4009_0002_0339.pdf;
16.2. příloha – 2019_01_18_4009_0043_0412.pdf;
16.3. příloha – 2019_01_19_4009_0042_8168.pdf;
16.4. příloha – 2019_02_11_4006_0018_3920.pdf;
16.5. příloha – 2019_03_14_4009_0042_5149.pdf;
16.6. příloha – 2019_03_22_4009_0017_7235.pdf;
16.7. příloha – 2019_04_16_4009_0075_8836.pdf;
16.8. příloha – 2019_06_15_4009_0005_5251.pdf;
16.9. příloha – 2019_06_15_4009_0005_5252.pdf;
16.10. příloha – 2019_07_04_4009_0042_0007.pdf;
16.11. příloha – 2019_07_09_4009_0043_8256.pdf;
16.12. příloha – 2019_08_14_4009_0042_6902.pdf;
16.13. příloha – 2019_08_15_4009_0007_9656.pdf;
16.14. příloha – 2019_08_30_4009_0044_2525.pdf;
16.15. příloha – 2019_08_30_4009_0044_2526.pdf;
16.16. příloha – 2019_10_08_4009_0007_9618.pdf;
16.17. příloha – 2019_10_23_4009_0042_7673.pdf;
16.18. příloha – 2019_11_22_4009_0042_2259.pdf;
16.19. příloha – 2020_01_11_4009_0042_9754.pdf;
16.20. příloha – 2020_01_18_4009_0044_6587.pdf;
16.21. příloha – 2020_01_23_4009_0002_5464.pdf;
16.22. příloha – 2020_01_23_4009_0003_0480.pdf;
16.23. příloha – 2020_02_01_4009_0018_7953.pdf;

16.24. příloha – 2020_02_14_4009_0042_5130.pdf;
16.25. příloha – 2020_02_14_4009_0044_1254.pdf;
16.26. příloha – 2020_02_17_4009_0042_5629.pdf;
16.27. příloha – 2020_02_22_4009_0086_2518.pdf;
16.28. příloha – 2020_03_20_4009_0084_0871.pdf;
16.29. příloha – 2020_03_21_4009_0081_5963.pdf;
16.30. příloha – 2020_04_27_4009_0048_6226.pdf;
16.31. příloha – 2020_04_27_4009_0048_6227.pdf;
16.32. příloha – 2020_04_27_4009_0078_3580.pdf;
16.33. příloha – 2020_04_30_4009_0046_9905.pdf;
16.34. příloha – 2020_05_07_4009_0081_9315.pdf;
16.35. příloha – 2020_05_16_4009_0086_3967.pdf;
16.36. příloha – 2020_07_05_4009_0069_6170.pdf;
16.37. příloha – 2020_07_15_4009_0042_6716.pdf;
16.38. příloha – 2020_07_19_4009_0045_2353.pdf;
16.39. příloha – 2020_07_20_4009_0048_7501.pdf;
16.40. příloha – 2020_07_29_4009_0083_5007.pdf;
16.41. příloha – 2020_08_14_4009_0069_1416.pdf;
16.42. příloha – 2020_08_28_4009_0042_4103.pdf;
16.43. příloha – 2020_09_10_4009_0069_4396.pdf;
16.44. příloha – 2020_09_11_4009_0043_9498.pdf;
16.45. příloha – 2020_09_26_4009_0044_1481.pdf;
16.46. příloha – 2020_10_27_4009_0049_3693.pdf;
16.47. příloha – 2020_10_27_4009_0049_3694.pdf;
16.48. příloha – 2020_11_07_4009_0014_6699.pdf;
16.49. příloha – 2020_11_07_4009_0017_5655.pdf;
16.50. příloha – 2020_11_09_4009_0082_0579.pdf;
16.51. příloha – 2020_11_16_4009_0083_3349.pdf;
16.52. příloha – 2020_11_23_4009_0069_2815.pdf;
16.53. příloha – 2020_12_11_4009_0069_5514.pdf;
16.54. příloha – 2020_12_18_4009_0012_8857.pdf;
16.55. příloha – 2021_01_22_4009_0081_5551.pdf;
16.56. příloha – 2021_02_11_4009_0085_4789.pdf;
16.57. příloha – 2021_02_11_4009_0085_4790.pdf;
16.58. příloha – 2021_03_06_4009_0084_2801.pdf;
16.59. příloha – 2021_03_15_4009_0084_4325.pdf;
16.60. příloha – 2021_03_20_4009_0086_8139.pdf;
16.61. příloha – 2021_04_03_4009_0085_4914.pdf;
16.62. příloha – 2021_05_07_4009_0087_0010.pdf;

17. Úřední záznam o pořízení dokumentace ze dne 27. května 2021, čj. UOOU-00807/21-23, počet stran 1;
    17.1. příloha – Informace o cookies, počet stran 6
    17.2. příloha – Další informace o cookies na www.allaboutcookies.org, počet stran 6;
    17.3. příloha – Zapnutí a vypnutí souboru cookie (u prohlížeče Chrome nebo Safari), počet stran 2;
    17.4. příloha – Informace o zpracování a ochraně osobních údajů společností XXXXX, počet stran 3;
    17.5. příloha – Seznam zpracovatelů, počet stran 1;

17.6. příloha – Informace o zpracování osobních údajů kamerovým systémem, počet stran 1;
17.7. příloha – Jaké cookies zpracováváme, počet stran 1.

18. Úřední záznam o pořízení dokumentace ze dne 10. června 2021, čj. UOOU-00807/21-24, počet stran 1;
18.1. příloha – Oznámení pověřence pro ochranu osobních údajů kontrolované osoby, počet stran 1;
18.2. příloha – Všeobecné podmínky věrnostního programu XXXXXXX 1. května 2021, počet stran 7;
19. Protokol o z ústního jednání ze dne 16. června 2021, čj. UOOU-00807/21-25, počet stran 4;
20. Vyjádření kontrolované osoby ze dne 29. června 2021 (Prezentace_GDPR_pro_Vedoucí_zaměstnance), čj. UOOU-00807/21-26, počet stran 27;
21. Vyjádření kontrolované osoby ze dne 25. června 2021, čj. UOOU-00807/21-27, počet stran 5;
21.1. příloha – P1_Cteci_logy_Náhledy_z_aplikace.pdf, počet stran 3;
21.2. příloha – P1_Cteci_logy_Přehled_záznamů_přístupů_zaměstnanců.xlsx, počet stran 3;
21.3. příloha – P2_XXXXX_Skartace.pdf, počet stran 1;
21.4. příloha – P3_Cookies_XX.xlsx, počet stran 4;
21.5. příloha – P4_GDD_Kontrola_procesů.pdf, počet stran 1;
21.6. příloha - P4_XXXXX_Zaznam_o_kontrole_opravneni_pristupu_k_ou_2021_04_30_3.pdf, počet stran 4;
21.7. příloha - P4_XXXXXX_Project_Security_Card_Záznam_o_činnostech_zpracování_CZE_.pdf, počet stran 2;
21.8. příloha – P4_XXXXX_GDPR_prohlášení_XXXX_podepsane.pdf, počet stran 3;
21.9. příloha – P4_XX_GDPR_zprava_pro_XXXXX_012021.pdf, počet stran 3;
21.10. příloha – P4_XX_cert_ISO_9001_CZ_issue_6.pdf, počet stran 1;
21.11. příloha – P4_XX_cert_ISO_27001_CZ_issue_5.pdf, počet stran 1;
21.12. příloha – P4_XX_potvrzeni_o_skoleni_zamestnancu_GDPR_012021.pdf, počet stran 1;
21.13. příloha – P5_XXXXXX_18_5_07.pdf, počet stran 1;
21.14. příloha – P5_Komunikace_XXXX.pdf, počet stran 7;
21.15. příloha – P6_Elektornické_školení_kvíz.pdf, počet stran 6;
21.16. příloha – P6_Elektronické_školení.pdf, počet stran 5;
21.17. příloha – P6_GDPR_5tero_pro_Nevedoucí_zaměstnance.docx, počet stran 1;
21.18. příloha – P6_GDPR_Kvíz_zaměstnanci_na_hypermarketech.docx, počet stran 1;
21.19. příloha – P6_Prezentace_GDPR_pro_Vedoucí_zaměstnance.pdf, počet stran 27;
22. P1_Cteci_logy_Náhledy_z_aplikace.pdf, počet stran 3;
22.1. příloha – P1_Cteci_logy_Přehled_záznamů_přístupů_zaměstnanců.xlsx, počet stran 3;
22.2. příloha – P2_XXXXX_Skartace.pdf, počet stran 1;
22.3. příloha – P3_Cookies_XX.xlsx, počet stran 4;
22.4. příloha – P4_XXX_Kontrola_procesů.pdf, počet stran 1;

22.5. příloha - P4_XXX_Zaznam_o_kontrole_opravneni_pristupu_k_ou_2021_04_30_3.pdf, počet stran 4;
22.6. příloha - P4_XXXXXX_Project_Security_Card_Záznam_o_činnostech_zpracování_CZE_.pdf, počet stran 2;
22.7. příloha – P4_XXXX_GDPR_prohlášení_XXXXXX_podepsane.pdf, počet stran 3;
22.8. příloha – P4 XX_GDPR_zprava_pro XXXXX_012021.pdf, počet stran 3;
22.9. příloha – P4_XX_cert_ISO_9001_CZ_issue_6.pdf, počet stran 1;
22.10. příloha – P4_XX_cert_ISO_27001_CZ_issue_5.pdf, počet stran 1;
22.11. příloha – P4_WT_potvrzeni_o_skoleni_zamestnancu_GDPR_012021.pdf, počet stran 1;
22.12. příloha – P5_XXXX_18_5_07.pdf, počet stran 1;
22.13. příloha – P5_Komunikace_XXXX.pdf, počet stran 7;
22.14. příloha – P6_Elektornické_školení_kvíz.pdf, počet stran 6;
22.15. příloha – P6_Elektronické_školení.pdf, počet stran 5;
22.16. příloha – P6_GDPR_5tero_pro_Nevedoucí_zaměstnance.docx, počet stran 1;
22.17. příloha – P6_GDPR_Kvíz_zaměstnanci_na_hypermarketech.docx, počet stran 1;
22.18. příloha – P6_Prezentace_GDPR_pro_Vedoucí_zaměstnance.pdf, počet stran 27;

23. Úřední záznam o pořízení dokumentace ze dne 1. července 2021, čj. UOOU-00807/21-29, počet stran 1;
23.1. příloha – Oznámení pověřence pro ochranu osobních údajů kontrolované osoby, počet stran 1.

V rámci kontroly je posuzováno výhradně zpracování osobních údajů v rozsahu stanoveném v předmětu kontroly, a ledaže je níže uvedeno jinak, v čase provedení kontroly. Z výše uvedených podkladů jsou pro kontrolní zjištění v protokolu o kontrole výslovně vyhodnoceny pouze ty podklady, případně jejich části, v nichž jsou uvedeny relevantní informace.

II. Důvod kontroly:

Kontrola byla zahájena na základě kontrolního plánu Úřadu pro rok 2021, zaměřila se především na dodržování zásad zpracování osobních údajů dle čl. 5 (minimalizace, omezení uložení a integrita a důvěrnost), zákonnosti zpracování osobních údajů podle čl. 6 (včetně případného profilování), podmínky udělení souhlasu se zpracováním osobních údajů 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 a zabezpečení zpracování podle čl. 32 (zabezpečení databáze zákazníků) nařízení (EU) 2016/679.

III. Kontrolní zjištění:

Společnost pořádá pro své zákazníky věrnostní program (dále jen „VP“), který probíhá v jeho prodejnách a on-line obchodě. Je zaměřen na poskytování nadstandardních výhod pro stálé zákazníky společnosti (dále také „člen VP“). Členství je určeno fyzickým osobám starším 18 let, je bezplatné, vzniká provedením registrace. Mimi klub je součástí, podprogramem VP. Níže popsaná kontrolní zjištění jsou zaměřená na zpracování osobních údajů registrovaných členů VP.

Kontrolní zjištění č. 1:

Kontrolující předně posuzovali, zda informace, které kontrolovaná osoba v souvislosti s VP zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, podle kterého se osobním údajem 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“*.

Podle čl. 4 bod 2 nařízení (EU) 2016/679 se zpracováním rozumí *jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, 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 osobní údaje o členech VP jsou zpracovávány v následujících evidencích:I, II, III a v papírových registračních formulářích.

I. je hlavní databáze, kde jsou uchovávány osobní údaje členů VP, kteří se registrovali do VP – účelem je zajištění řádného fungování VP. V této databázi jsou osobní údaje zpracovávány v následujícím rozsahu: jméno, příjmení, datum narození (nepovinný údaj), pohlaví (jen u elektronického formuláře), adresa, telefonní číslo (v případě nevyplnění e-mailové adresy), e-mailová adresa, ID sociální sítě (nepovinný údaj, jen u elektronického formuláře), EAN a číslo zákaznické karty, domovský hypermarket, počet členů domácnosti (nepovinný údaj), údaje o nákupním chování.

V případě registrace v Mimi klubu jsou pak zpracovávány osobní údaje v tomto rozsahu: předpokládaný termín porodu (jen v papírovém formuláři), jméno dítěte, pohlaví (jen u elektronického formuláře) a datum narození dětí.

II. je databáze, ve které jsou evidovány pouze osobní údaje ve tvaru ID zákazníka (pořadové číslo registrace) a jemu přidělené kupony.

III. slouží k vedení přehledu kontaktů registrovaných zákazníků, členů VP, které jsou provázané v I., k zasílání reklamních letáků a zpracovávají se v ní osobní údaje v rozsahu telefonní číslo a emailová adresa.

Poslední databází, kterou společnost v souvislosti s předmětem kontroly zpracovává jsou papírové registrační formuláře. V těchto jsou zpracovávané osobní údaje v rozsahu: jméno, příjmení, adresa, telefonní číslo, e-mailová adresa, EAN a číslo zákaznické karty, domovský hypermarket XXXX, podpis, datum narození a počet členů domácnosti jako nepovinný údaj a v případě Mimi klubu: jméno, předpokládaný termín porodu, datum narození dětí. (podklad č. 3.1.)

Osobní údaje jsou od členů VP získávány (shromažďovány) jak v listinné podobě (papírové registrační formuláře), tak v elektronické podobě (elektronický registrační formulář – on-line registrace na webových stránkách.

V papírovém formuláři jsou požadovány tyto osobní údaje
jako povinné:

- jméno a příjmení;
- adresa (bez země);
- e-mailová adresa nebo telefonní číslo;
- EAN a číslo zákaznické karty;
- domovský hypermarket XXXXX;
- datum podpisu formuláře;
- podpis;

jako nepovinné:

- datum narození;
- počet členů domácnosti.

V elektronickém formuláři na webových stránkách společnosti jsou požadovány tyto osobní údaje
jako povinné:

- jméno a příjmení;
- adresa (včetně země);
- e-mailová adresa;
- heslo;
- v případě registrace prostřednictvím účtu na sociální síti Facebook či Google – ID uživatele zvolené sítě;

a jako nepovinné:

- datum narození
- pohlaví
- telefonní číslo.

Při on-line nákupu jsou po přihlášení člena VP prostřednictvím webové stránky zpracovávány tyto osobní údaje: identifikační údaje, kontaktní údaje, produktové údaje (EAN zákaznické karty, číslo zákazníka), komunikační údaje (logy, připomínky, přání, žádosti a chování zákazníka), profilové osobní údaje (IP adresa, cookies) a údaje o objednávkách (artikly (ID, cena, množství).

Po odevzdání řádně vyplněného papírového registračního formuláře v infomačním centru hypermarketu je zájemci předána členská karta, která mu umožní využívat všechny funkce spojené s VP.

Po vyplnění elektronického formuláře je následně zájemci (na e-mailovou adresu uvedenou ve formuláři) odeslán potvrzující e-mail s aktivačním odkazem. Kliknutím na tento aktivační odkaz zájemce dokončí proces registrace a zpět obdrží registrační kód. S tímto kódem se zájemce dostaví do informačního centra hypermarketu, kde mu je předána karta, která mu umožní využívat všechny výhody spojené s VP. Nedokončí-li zájemce registraci nejpozději do 2 měsíců od doručení e-mailu s aktivačním odkazem, je proces registrace zájemce

ukončen, přičemž údaje zájemce uvedené v registračním formuláři nejsou společností dále evidovány či jinak zpracovávány.

Kontrolující proto vyhodnotili zjištěný stav věci tak, že informace, které kontrolovaná osoba o svých členech VP zpracovává, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679.

Soubory operací, které jsou u kontrolované osoby prováděny s osobními údaji členů VP (jako např. shromažďování, ukládání, oprava a úprava osobních údajů, analýza, uchovávání osobních údajů, likvidace), jsou zpracováním osobních údajů ve smyslu čl. 4 bod 2 nařízení (EU) 2016/679.

Kontrolní zjištění č. 2:

Kontrolující následně posuzovali postavení kontrolované osoby ve vztahu k čl. 4 bodu 7 nařízení (EU) 2016/679, dle kterého se správcem 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.“*

K postavení kontrolované osoby ve vztahu k osobním údajům členů VP, je nezbytné posoudit, zda společnost stanovila účel a prostředky jejich zpracování.

Jak vyplývá z definice uvedené v úvodu tohoto kontrolního zjištění, pro určení postavení správce osobních údajů je rozhodující skutečností určení účelu a prostředků zpracování osobních údajů.

V podkladech k předmětné kontrole jsou *v Záznamech o činnostech zpracování osobních údajů* a dokumentu *Informace o ochraně osobních údajů* uvedeny následující účely zpracování osobních údajů:

- zajištění provozu VP, zajištění personalizace jednotlivých emailových rozesílek, příprava reportů a jiných analýz;
- registrace členů VP;
- ochrana oprávněných zájmů společnosti (určení, výkon a obhajoba případných právních nároků);
- vedení záznamů o přidělených kuponech;
- zasílání reklamních letáků;
- ověření zákazníka, oprava/úprava jeho osobních údajů;
- nahrání CSV souboru do nástroje na rozesílání SMS, rozeslání SMS zpráv;
- realizace marketingových aktivit v rámci VP;
- vytváření průzkumů, analýz a obchodních statistik ohledně nákupního chování a chování v rámci VP a obchodních statistik, s cílem vhodného přizpůsobení nabídky produktů a zkvalitnění poskytovaných služeb;
- zasílání obchodních sdělení a pozvánek na akce;
- poskytování odborných a marketingových informací.

Registrace zájemce o členství ve VP je prováděna prostřednictvím registračních formulářů, z nichž jsou osobní údaje dále zpracovávány způsobem a za účely, které jsou popsány (viz výše) a dále v kontrolním zjištění č. 1.

Kontrolující s ohledem na uvedené konstatují, že společnost je v postavení správce podle čl. 4 bodu 7 nařízení (EU) 2016/679, neboť určila způsob a prostředky předmětného zpracování osobních údajů.

Kontrolní zjištění č. 3:

Kontrolující se zabývali skutečností, zda zpracování osobních údajů, které je předmětem této kontroly, probíhá v souladu s čl. 6 nařízení (EU) 2016/679, podle kterého musí správce osobních údajů vždy disponovat legitimním právním titulem pro zpracování osobních údajů.

Podle čl. 6 odst. 1 nařízení (EU) 2016/679 *„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.“

Výše uvedené ustanovení tak reflektuje jednu ze základních zásad zpracování osobních údajů, která je uvedena v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679, tedy zásadu zákonnosti – *„Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“)“.*

Společnost zpracovává předmětné osobní údaje členů VP na základě vícero právních titulů, které vyplývají z výše uvedeného článku nařízení.

VP pořádaný společností, je zaměřen na poskytování nadstandardních výhod pro členy VP. Členství v programu je bezplatné a vzniká registrací, tedy se souhlasem fyzické osoby starší 18 let.

Každý člen VP uděluje společně s registrací do VP svůj souhlas, aby po dobu trvání jeho členství ve VP, nejdéle však do odvolání souhlasu, společnost zpracovávala jeho osobní údaje a případně údaje dětí vyplněné v registračním formuláři.

Souhlas se zpracováním osobních údajů je člen VP oprávněn kdykoli odvolat. Doručením odvolání souhlasu se zpracováním osobních údajů pozbude společnost oprávnění zpracovávat osobní údaje člena VP pro účely uvedené v souhlasu se zpracováním osobních údajů.

Společnost tedy zpracovává osobní údaje členů VP na základě souhlasu, právního titulu, který je stanoven v čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679. Dle čl. 4 odst. 11 tohoto nařízení je *„souhlasem subjektu údajů jakýkoli svobodný, konkrétní informovaný a jednoznačný projev vůl, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování osobních údajů*“. Dle čl. 7 *musí být správce schopen souhlas subjektu údajů doložit, subjekt údajů má právo svůj souhlas kdykoli odvolat“.*

Souhlas je při registraci zákazníka do VP součástí papírového formuláře na straně 5, v elektronickém formuláři pod tímto konkrétním odkazem na webu společnosti. Oba texty souhlasů jsou shodné, a to v následujícím znění: *„Uděluji společnosti souhlas se zpracováním osobních údajů v rozsahu registračního formuláře (pro případ registrace a/nebo přihlašování do uživatelského účtu prostřednictvím sociální sítě také se zpracováním ID uživatele zvolené sociální sítě) a se sběrem a zpracováním informací vztahujících se k mému nákupnímu chování, shromážděných v rámci provozování věrnostního programu (dále jen „věrnostní program“ a „osobní údaje“). Pokud se účastním podprogramu Mimi klub, souhlasím též se zpracováním osobních údajů dětí v rozsahu registračního formuláře, a to i po ukončení členství v tomto podprogramu.*

Na základě tohoto souhlasu je společnost oprávněna zpracovávat osobní údaje za účelem realizace marketingových aktivit v rámci věrnostního programu, vytváření průzkumů a obchodních statistik ohledně nákupního chování a chování v rámci věrnostního programu, zasílání obchodních sdělení a pozvánek na akce pořádané společností (včetně zasílání obchodních sdělení elektronickými prostředky) a poskytování odborných a marketingových informací, to vše jakýmikoliv prostředky komunikace (zejména e-mailem, telefonicky, SMS zprávami a poštou).

Dále uděluji souhlas s tím, že společnost může osobní údaje zpracovávat za použití výhradně automatizovaných postupů, které pro mne mohou mít právní účinky nebo se mne mohou obdobným způsobem významně dotýkat (automatizované rozhodování). To znamená, že při použití uvedených postupů mohou být osobní údaje automaticky zpracovávány takovým způsobem, aby byly členům věrnostního programu poskytovány výhody a nabídky odpovídající jejich preferencím a/nebo zájmům dle zjištěného nákupního chování. V důsledku automatizovaného rozhodování mohou jednotliví členové věrnostního programu obdržet odlišné výhody a nabídky, případně některé poskytované nabídky a/nebo výhody mohou být dostupné pouze vybraným členům věrnostního programu.
Tento souhlas uděluji na dobu trvání mého členství ve věrnostním programu, nejdéle však do doby jeho odvolání, což mohu učinit kdykoliv.

Udělením tohoto souhlasu současně potvrzuji, že jsem se seznámil/seznámila s Informacemi o ochraně osobních údajů a se všemi právy, které mi v souvislosti se zpracováním osobních údajů společnosti náleží.“

Součástí obou výše uvedených způsobů registrace jsou následující závěrečná ujednání:

„Po pečlivém seznámení s Informacemi o ochraně osobních údajů (str. 3) a Úplným zněním souhlasu se zpracováním osobních údajů člena programu společnosti (str. 5) (dále jen „Úplné znění souhlasu“) souhlasím se zpracováním všech mnou výše uvedených osobních údajů o mé osobě a popřípadě i o mnou registrovaných dětech, v rozsahu Úplného znění souhlasu, tedy se zpracováním osobních údajů společností“

- *„za účelem realizace marketingových aktivit v rámci věrnostního programu, vytváření průzkumů a obchodních statistik, zasílání obchodních sdělení a pozvánek na akce a poskytování odborných a marketingových informací;“*
- *„za užití výhradně automatizovaných postupů, které pro mne mohou mít právní účinky nebo se mne mohou obdobným způsobem významně dotýkat; v důsledku toho bude XXXX schopen poskytovat personalizované výhody a nabídky.“*

„S ohledem na zvláštní povahu věrnostního programu nezaregistruje zájemce do programu, nebudou-li oba výše uvedené souhlasy uděleny. Zákazník má však i nadále možnost nakupovat zboží a využívat služby společnosti.“ V papírovém formuláři je tato informace zřetelně zobrazena v části závěrečných ujednání, oproti tomu v elektronickém formuláři se tato informace zobrazí pouze pokud zákazník najede myší na symbol otazníku vedle výše uvedených závěrečných ujednání.

„Souhlasím s Všeobecnými podmínkami věrnostního programu, s nimiž jsem se před podpisem tohoto registračního formuláře pečlivě seznámil/a, a potvrzuji, že jsem k dnešnímu dni dosáhl/a věku 18 let.“ Všeobecné podmínky VP, nejsou součástí papírového registračního formuláře oproti elektronickému formuláři, kde je na uvedené podmínky odkaz.

Společnost si stanovila postupy, kterými má subjekt údajů možnost odvolat souhlas, konkrétně: elektronicky na webových stránkách společnosti, na konkrétní e-mailové adrese nebo písemně na kontaktních místech společnosti.

Takto udělený souhlas tedy splňuje požadavky, které na souhlas se zpracováním osobních údajů nařízení (EU) 2016/679 klade.

Dále společnost zpracovává osobní údaje členů VP za účelem:

- plnění práv a povinností plynoucích z uzavřených smluv a/nebo objednávek učiněných zákazníkem (osobní údaje jsou zpracovávány po dobu trvání práv a povinností z kupní smlouvy/objednávky, nejdéle však po dobu 5 let);
- oprávněných zájmů při zajištění ochrany osob a majetku v prostorách provozoven společnosti (kontrolovaná osoba snímá některé venkovní i vnitřní prostory svých provozoven pomocí kamerového systému);
- plnění povinností uložených společnosti právními předpisy (jedná se zejména o účetní a daňové povinnosti);
- také zajištění řádného fungování internetových stránek;
- nebo informování zákazníků o aktivitách společnosti.

Kontrolou bylo zjištěno, že společnost zpracovává osobní údaje členů VP na základě následujících právních titulů:

- souhlas se zpracováním osobních údajů dle čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679, který zákazníci udělují při registraci do VP;
- zajištění řádného fungování VP a plnění práv a povinností společnosti vůči členům VP dle čl. 6 odst. 1 písm. b) nařízení (EU) 2016/679;
- plnění právních povinností kontrolované osoby dle čl. 6 odst. 1 písm. c) nařízení (EU) 2016/679;
- ochrana oprávněných zájmů společnosti dle čl. 6 odst. 1 písm. f) nařízení (EU) 2016/679.

Kontrolující vyhodnotili zjištěný stav tak, že kontrolovaná osoba **neporušila** povinnost stanovenou v čl. 6 odst. 1 písm. a), b), c) a f) nařízení (EU) 2016/679, tedy že zpracování osobních údajů je založeno na legitimních právních titulech.

Kontrolní zjištění č. 4:

Kontrolující taktéž posuzovali, jakým způsobem dochází k naplňování zásad ve smyslu čl. 5 odst. 1 konkrétně písm. a), c) - e) nařízení (EU) 2016/679. Podle uvedeného článku nařízení (EU) 2016/679 *„Osobní údaje musí být:*

a) ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“);

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 přihlédnut m 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 nařízen m s cílem zaručit práva a svobody subjektu údajů („omezení uložení“);“

Zásada čl. 5 odst. 1 písm. a) je jedním z hlavních projevů zásady zákonnosti (správce může osobní údaje zpracovávat pouze v případě, kdy k tomu má alespoň jeden z právních titulů, které jsou stanoveny v čl. 6 odst. 1 písm. a) - f) nařízení (EU) 2016/679. Dle čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679 *„Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“)“.* Jak kontrolující konstatovali v kontrolním zjištění č. 2 kontrolovaná osoba tuto povinnost splnila.

Kontrolovaná osoba dodržela povinnosti stanovené v čl. 5 odst. 1 písm. a) nařízení (EU) 2016/679 a tudíž splnila uvedené ustanovení.

V souvislosti se zásadou minimalizace údajů (čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679 kontrolující zhodnotili rozsah osobních údajů, které společnost zpracovává v rámci realizace VP. Tento rozsah, je popsán v kontrolním zjištění č. 1. společnost zpracovává pouze údaje vztahující se k účelům, které stanovil, kontrolující tedy zhodnotili tento stav tak, že kontrolovaná osoba splnila zásadu minimalizace osobních údajů.

Společnost se v průběhu kontroly rozhodla při elektronické registraci do programu VP nadále nepožadovat nepovinný údaj „pohlaví".

Kontrolovaná osoba splnila povinnosti stanovené v čl. 5 odst. 1 písm. c) nařízení (EU) 2016/679.

V kontextu se zásadou přesnosti (čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679), kontrolující prověřili, jak dochází k aktualizaci osobních údajů členů VP. V dokumentu Všeobecné podmínky VP v sekci XX. je uvedeno, že *„člen programu bere na vědomí, že dojde-li k jakékoli změně údajů, které uvedl při registraci, je povinen tuto změnu společnosti neprodleně oznámit, a to ohlášením změny na infolince nebo změnou v registračních údajích člena programu na svém členském účtu"*. Člen VP, se tedy zavazuje k tomu, že v případě změny relevantních osobních údajů, sám kontaktuje kontrolovanou osobu a tyto osobní údaje aktualizuje.

Kontrolou bylo také ověřeno, že členové VP, kteří uvedli údaje o plánovaném datu porodu dítěte, jsou k tomuto datu dotázáni prostřednictvím e-mailu, zda sdělí skutečné datum narození dítěte. Bez ohledu na to, zda skutečné datum porodu sdělí, není údaj o plánovaném datu porodu kontrolovanou osobou dále zpracováván.

Kontrolovaná osoba splnila povinnosti stanovené v čl. 5 odst. 1 písm. d) nařízení (EU) 2016/679.

Dle čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679 by měly být osobní údaje uloženy ve formě umožňující identifikaci subjektu údajů po dobu ne delší, než je nezbytné pro účely, pro které jsou zpracovávány (zásada uchování). Ve Všeobecných podmínkách VP kontrolovaná osoba uvádí, že osobní údaje členů VP bude zpracovávat po dobu trvání členství v VP, nejdéle však do odvolání souhlasu.

Papírové registrační formuláře vyplněné zájemci o registraci do VP jsou uchovávány po dobu 3 měsíců od jejich přepsání do elektronické podoby. Následně jsou zlikvidovány spálením. Likvidaci papírových registračních formulářů zpracovává Infolinka. Kontrolovaná osoba doložila potvrzení o skartaci formulářů.

Dle vyjádření společnosti osobní údaje týkající se nákupního chování členů VP (identifikační kód hypermarketu, datum nákupu, EAN zákaznické karty, název, cena a množství zakoupeného artiklu, výše nákupu a historie bonusů) zpracovávají po dobu 3 let. Po uplynutí uvedené doby jsou tyto údaje smazány z datového serveru, a nadále zůstávají uchovávány daňové a účetní doklady po dobu předepsanou zvláštními právními předpisy.

Osobní údaje týkající se on-line nákupu uvedené v kontrolním zjištění č. 1 společnost uchovává po dobu 3 let, tedy shodně s údaji získanými při nákupu v hypermarketu.

Kontrolující mají za to, že takto určená doba zpracování prováděného v souvislosti s uskutečněnými nákupy členů VP (nákupní chování a online nákupy) je nepřiměřená, zejména pak s ohledem na to, že ve velkém množství případů se jedná o údaje o nákupu potravinářského zboží.

Vzhledem k výše uvedenému by kontrolovaná osoba měla omezit dobu zpracování osobních údajů, a to podle účelu, pro který jsou osobní údaje zpracovávány, např. v případě záznamů o zakoupeném zboží na dobu, kdy je možné u tohoto zboží uplatnit reklamaci, nebo na dobu kdy je potřeba tyto údaje zpracovávat pro marketingové účely.

Kontrolovaná osoba **porušila** povinnost stanovenou v čl. 5 odst. 1 písm. e) nařízení (EU) 2016/679 a tudíž **porušila** uvedené ustanovení.

Kontrolní zjištění č. 5:

Kontrolující se dále zaměřili na posouzení plnění povinnosti uvedené v ustanovení čl. 12 nařízení (EU) 2016/679, v rozsahu informace dle čl. 13 a 14 tohoto nařízení. Uvedená ustanovení upravují povinnost správce informovat subjekt údajů o všech podstatných parametrech zpracování osobních údajů, a to včetně jeho práv, která mu ve vztahu k tomuto zpracování vznikají.

Podle čl. 12 nařízení (EU) 2016/679 *„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 čl. 13 a 14 nařízení (EU) 2016/679.“*

Podle čl. 13 a 14 nařízení (EU) 2016/679 je správce při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Povinnost dle citovaného zákonného ustanovení je povinen správce splnit před zpracováním osobních údajů subjektů údajů.

Pro splnění informační povinnosti je rozhodná skutečnost, zda osobní údaje byly správci osobních údajů poskytnuty přímo subjektem údajů (čl. 13), nebo je správce získal od jiného než od subjektu údajů (čl. 14). Vzhledem k tomu, že společnost získává osobní údaje přímo od zákazníků (subjektu údajů), je povinna mu podat informace o zpracování jeho osobních údajů podle čl. 13 nařízení 2016/679.

Společnost poskytuje informační povinnost několika způsoby – prostřednictvím telefonní infolinky společnosti, dále v písemné i elektronické podobě.

Informační povinnost je naplňována prostřednictvím dokumentů, která jsou součástí webových stránek společnosti (dokumenty 1 – 3).

add 1. Je základním informačním materiálem pro všechny zákazníky, v jehož jednotlivých částech jsou následující informace o zpracování osobních údajů zákazníků:

- o společnosti jako správci, o oprávnění společnosti ke zpracování osobních údajů, k jejich předávání, o technicko-organizačních opatřeních, které byly společností přijaty za účelem zabezpečení těchto údajů (ochrana před neoprávněnou manipulací, ztrátou, zničením nebo přístupem nepovolaných osob);
- o uplatnění práv v souvislosti se zpracováním osobních údajů a o možnosti zrušení elektronických obchodních sdělení prostřednictvím odkazu obsaženém v každém jednotlivém obchodním sdělení.

add 2. Je zákazníkům předkládána jako součást papírového formuláře při registraci. Při on-line registraci jsou zákazníkovi tyto informace poskytnuty v registračním kroku jako odkaz na webu a zároveň je zveřejněn na webové stránce společnosti. Uvedená informace je rozčleněna do několika částí (osobní údaje, oprávnění společnosti ke zpracování osobních údajů, předávání osobních údajů a práva členů VP):
   - informace o rozsahu zpracování osobních údajů zákazníků (kontaktní a identifikační údaje, nákupní chování, které jsou součástí registračního formuláře v listinné nebo elektronické podobě;
   - popis průběhu registrace do VP prostřednictvím elektronického formuláře ze zvolené sociální sítě;
   - subjekty údajů jsou informováni kromě samotných oprávnění také o automatizovaném zpracování a rozhodování;
   - společnost uvádí možnost pověření zpracováním osobních údajů zpracovateli v České republice i v zahraničí; informuje, že osobní údaje mohou být předány zejména poskytovatelům IT služeb, logistických služeb, marketingovým agenturám, provozovatelům call center a poskytovatelům poštovních a doručovacích služeb. Odkazuje na seznam zpracovatelů, který je k dispozici na vyžádání na kontaktních místech společnosti a na jejích webových stránkách;
   - kromě vyjmenovaných práv, poskytuje informace o možných způsobech odvolání souhlasu, o zrušení přijímání elektronických obchodních sdělení, o infolince s informacemi ohledně ochrany osobních údajů, včetně informace, kde mohou členové VP uvedená práva uplatňovat (na kontaktních místech společnosti.

add 3. Jsou k dispozici na webové stránce společnosti nebo v listinné podobě k nahlédnutí v písemné podobě na informacích v jednotlivých marketech a popisují například celý registrační proces včetně podmínek k provedení registrace zákazníka; výhody VP; služby, které je možné v rámci VP využívat.

Společnost v textu Souhlasu se zpracováním osobních údajů v sekci, která se týká zpracování osobních údajů za účelem zařazení člena VP do jednotlivých úrovní členství („řád věrnosti“) a vytváření personalizovaných akčních uvádí: „*Dále uděluji souhlas s tím, že společnost může osobní údaje zpracovávat za použití výhradně automatizovaných postupů, které pro mne mohou mít právní účinky nebo se mne mohou obdobným způsobem významně dotýkat“,* tato informace může být zavádějící, jelikož zákazník tak může nabýt dojmu, že ze zpracování, které kontrolovaná osoba provádí výhradně automatizovanými postupy mohou vznikat právní účinky i když tomu tak není.

Kontrolou bylo také zjištěno, že pod termínem „nákupní chování“ zákazníků – členů VP, který je uveden v textu Souhlasu se zpracováním osobních údajů VP, společnost zpracovává informace v následujícím rozsahu: identifikační kód hypermarketu, datum nákupu, EAN zákaznické karty, název, cena a množství zakoupeného artiklu, výše nákupu a historie bonusů. Při udělení souhlasu však v uvedeném případě pojem „nákupní chování“ není v textu souhlasu ani v informacích o ochraně osobních údajů dostatečně definován a subjekt údajů tak nemá informace o tom, jaké osobní údaje jsou pod tímto pojmem zahrnuty.

V dokumentu *Informace o zpracování a ochraně osobních údajů společností* je uvedeno následující : „společnost *je i bez souhlasu členů věrnostního programu oprávněn zpracovávat jejich osobní údaje z titulu (i) zajištění řádného fungování věrnostního programu a plnění práv a povinností společností vůči členům věrnostního programu a (ii)jeho oprávněných zájmů (jako například zpracování osobních údajů pro statistické účely, informování zákazníků o aktivitách společnosti, inkaso pohledávek, předcházení hackerských útoků a podobně),* ***a to nejméně po dobu trvání členství ve věrnostním programu“***
Dle čl. 13 odst. 2 písm. a) nařízení (EU) 2016/679 pokud je to třeba, měl by být subjekt údajů informován i o době po kterou budou osobní údaje uloženy, nebo není-li to možné určit kritéria použitá pro stanovené této doby. S ohledem na povahu VP, kdy subjekt údajů může být jeho členem dlouhodobě, kontrolovaná osoba by měla členy informovat o tom, že údaje sledující jejich chování v rámci VP jsou pravidelně mazány/anonymizovány.

Kontrolovaná osoba tedy neplní dostatečně informační povinnost, jelikož nepodává subjektu údajů jasnou informaci o rozsahu zpracovávaných osobních údajů, možných následcích tohoto zpracování a době, po kterou budou jejich osobní údaje zpracovávány (viz. zpracování automatizovanými způsoby s možnými právními účinky a pojem nákupní chování).

Kontrolující proto vyhodnotili zjištěný stav tak, že kontrolovaná osoba **porušila** povinnost stanovenou v čl. 12 nařízení (EU) 2016/679, v rozsahu čl. 13 tohoto nařízení, tedy že není dostatečně plněna informační povinnost správce.

Proto kontrolující doporučují kontrolované osobě výše uvedený text, týkající se automatizovaných postupů změnit, a dále doplnit definici pojmu „nákupní chování“ do znění textu souhlasu, nebo informace o ochraně osobních údajů.

Kontrolní zjištění č. 6:

Kontrolou bylo zjištěno, že společnost v rámci provozování webových stránek využívá cookies, proto se kontrolující v rámci předmětné kontroly zaměřili i na právní titul pro takové zpracování, tedy získání souhlasu (náležitosti uděleného souhlasu, případně jeho odvolání souhlasu).

Soubory cookies jsou textové soubory, které poskytovatel internetových stránek umístí do počítače uživatele těchto stránek a může k nim mít při nové návštěvě stránek uživatelem znovu přístup, a to za účelem usnadnění prohlížení internetu (nebo poskytování jiných služeb informační společnosti) nebo zjednodušení transakcí. Tyto soubory umožňují internetové stránce, aby si průběžně „pamatovala“ činnosti uživatele nebo jeho chování či preference, mohou být také použity pro shromažďování informací ohledně online chování uživatelů

pro cílenou reklamu a marketing. Soubory cookies můžeme rozlišovat podle své životnosti (např. relační cookies a trvalé cookies) a další podle domény, ke které cookies patří (např. cookies prvních osob a cookies třetích osob).

Dle čl. 4 odst. 1 nařízení (EU) 2016/679 je osobním údajem i síťový identifikátor. Ze spojení čl. 4 bod 1 a rec. 30 nařízení (EU) 2016/679 lze jednoznačně dovodit, že za osobní údaj je nezbytné považovat též identifikátory cookies, které umožňují spojení s konkrétní fyzickou osobou. Informace, které správce prostřednictvím cookies získává jsou tedy osobními údaji, jelikož se jedná o údaje o identifikované, nebo identifikovatelné fyzické osobě a při jejich zpracování tak musí být naplněny požadavky nařízení (EU) 2016/679.

V podkladech ke kontrole jsou uvedeny cookies používané společností v souvislosti s VP, včetně jejich názvů, domén, popisu, využitého nástroje a dat.

Společnost v rámci provozu webových stránek využívá následující cookies:

- technické cookies, tedy cookies první strany, jsou krátkodobé. Zajišťují základní technickou funkčnost webu, tj. přihlašování, zapamatování si nastavení, využívání služeb apod;
- statistické cookies (např. Google Analytics) první či třetí strany, jsou dlouhodobé. Jsou využity ke generování anonymních statistik o používání webu;
- reklamní cookies první i třetí strany jsou využívány pro behaviorální cílení reklamy podle zájmů uživatele, tedy k cílenému zobrazování reklam uživatelům, kteří již dříve uvedenou webovou stránku navštívili. Lze proto shrnout, že kontrolovaná osoba využívá soubory cookies mimo jiné i pro remarketing.

Souhlas se zpracováním osobních údajů prostřednictvím cookies (čl. 5 odst. 3 Směrnice č.2002/58/ES) podléhá režimu souhlasu ve smyslu čl. 4 bod 11 nařízení (EU) 2016/679, musí se tedy jednat o projev vůle, který je svobodný, konkrétní, informovaný a jednoznačný, učiněn prohlášením nebo jiným zjevným potvrzením. V takovém případě musí správce osobních údajů rovněž dodržet podmínky vyjádření souhlasu stanovené čl. 7 nařízení (EU) 2016/679, tedy musí prokázat souhlas se zpracováním osobních údajů, a to po celou dobu takového zpracování.

Společnost má na webových stránkách umístěný odkaz s informační lištou o cookies.
Text informační lišty o cookies zní: *„Tyto stránky používají k poskytování služeb cookies. Pokračováním v prohlížení vyjadřujete souhlas s jejich používáním. Více informací“.* Součástí lišty je i tlačítko *„Souhlasím“.*
V odkazu *Více informací* je uvedena informace o zpracování osobních údajů v souvislosti s využíváním cookies

- účel jejich používání (k personalizaci stránek);
- fungování cookies;
- možnost nastavení cookies v jednotlivých prohlížečích, včetně odkazů na tyto možnosti (Firefox Mozilla a Android – nefungují);
- o využívaných souborech cookies (vydavatel/název cookies a doba uchování) např. Adform až 530 dní, Facebook až trvale, XXXXX až trvale, Google Analytics 2 roky, DoubleClick 2 roky;
- o Google Analytics.

Na základě kontrolního zjištění a dále pak dle vyjádření kontrolované osoby, je text v liště formulován nesprávně, neboť souhlas s používáním cookies je členem VP udělen až kliknutím na tlačítko „Souhlasím“.

Kontrolovaná osoba v informaci o zpracování osobních údajů prostřednictvím cookies v sekci „Umožnit/Zakázat Cookies uvádí, že uživatel může odmítnout cookies úpravou nastavení svého prohlížeče, v takovém případě uživatel současně odmítne všechny cookies, i cookies z jiných webových stránek. Dle recitálu 43 nařízení (EU) 2016/679 *„lze předpokládat, že souhlas není svobodný, není-li možné vyjádřit samostatný souhlas s jednotlivými operacemi zpracování osobních údajů, i když je to v daném případě vhodné“*. Kontrolovaná osoba by tedy měla dát uživatelům serveru možnost vybrat se kterými cookies souhlas udělí, a to zejména s ohledem na to, že na svých stránkách využívá i cookies třetích stran. Souhlas se zpracováním osobních údajů prostřednictvím cookies tedy není možné považovat za svobodný.

Dle čl. 4 bod 11 nařízení (EU) 2016/679 musí být udělený souhlas se zpracováním osobních údajů informovaný. Informace, tak jak ji společnost poskytuje na svých webových stránkách neobsahuje výčet osobních údajů, které jednotlivé cookies zpracovávají. Uživatel tak neví, jaké jeho osobní údaje budou prostřednictvím cookies kontrolovanou osobou, nebo třetí stranou zpracovávány.

Společnost v informaci o zpracování osobních údajů v souvislosti s využíváním cookies uvádí odkazy na webové stránky s obecnou definicí, co jsou cookies a popisem, jak s nimi nakládat, tyto stránky jsou však v anglickém jazyce. Kontrolující mají proto za to, že souhlas se zpracováním osobních údajů prostřednictvím cookies, tak jak jej kontrolovaná osoba nastavila není informovaným souhlasem.

Kontrolující vyhodnotili zjištěný stav tak, že souhlas se zpracováním osobních údajů prostřednictvím cookies, tak jak jej kontrolovaná osoba nastavila, nesplnila požadavky čl. 4 odst. 11 a čl. 7 nařízení (EU) 2016/679, neboť nebyly řádně splněny požadavky informace k takovému zpracování a souhlas k jednotlivým cookies nelze jednoduchým způsobem vyjádřit či odvolat).

Kontrolovaná osoba tak **porušila** ustanovení čl. 6 odst. 1 písm. a) nařízení (EU) 2016/679, jelikož zpracovává osobní údaje členů VP (uživatelů webových stránek) prostřednictvím souborů cookies bez řádného souhlasu subjektu údajů.

Kontrolní zjištění č. 7:

Kontrolující hodnotili rovněž splnění povinnosti stanovené v čl. 15-21 nařízení (EU) 2016/679. Podle těchto ustanovení má subjekt údajů právo na přístup k osobním údajům, tj. právo žádat a získat relevantní informace o zpracování jeho osobních údajů a rovněž právo vznést námitku.

Věcně příslušnou osobou pro vyřizování žádostí o výkon práv subjektů údajů je pověřenec pro ochranu osobních údajů. (podklad č. 18.1.)

Společnost obdržela za období od 24. července 2019 do 30. března 2021 tři žádosti dle čl. 15 nařízení (EU) 2016/679, včetně žádosti o opravu osobních údajů dle čl. 16 nařízení (EU) 2016/679 (podklad č. 6.1.)

Žádosti dle čl. 17 nařízení (EU) 2016/679 jsou obvykle spojeny s žádostmi o ukončení členství a s tím související vymazání osobních údajů, běžně jsou řešeny žadateli přímo prostřednictvím infolinky.

Společnost stanovila interními předpisy (směrnice *Zpracování a ochrana osobních údajů*, *Pokyny ke zpracování osobních údajů pro informační a reklamační pracovníky* a *Pokyny ke zpracování osobních údajů pro zaměstnance oddělení marketing a multichannel*) postupy pro vyřizování žádostí subjektů údajů podle čl. 15-21 nařízení (EU) 2016/679, konkrétně:

- člen VP může u společnosti uplatnit svá práva subjektu údajů některým z následujících způsobů: poštou, telefonicky, emailem nebo elektronicky v uživatelském účtu VP;
- pověřený pracovník přezkoumá žádost bez zbytečného odkladu;
- jsou-li důvodné pochybnosti o totožnosti člena VP, je požádán o dodatečné informace pro provedení řádné identifikace;
- v případě výmazu osobních údajů žadatele, zadá pověřený pracovník příkaz k výmazu dotčených osobních údajů člena VP z relevantních databází. Pověřený pracovník vyrozumí člena VP o výsledcích uplatnění jeho práva bezodkladně, nejpozději však do jednoho měsíce od přijetí žádosti;
- osobní údaje dětí (pokud jsou zpracovávány) jsou vymazány spolu s ukončením členství zákazníka. Automaticky současně dojde k zadání příkazu k výmazu dotčených osobních údajů z databáze zpracovatele, pokud je to relevantní;
- v souvislosti s ukončením členství ve VP je také zablokovaná členská karta, kterou lze použít k platební funkci do vyčerpání všech peněžních bonusů či do data uplynutí platnosti posledního peněžního bonusu, tj. maximálně po dobu 12 měsíců od ukončení členství. Po 12 měsících exspirují všechny nevyčerpané bonusy a karta je ukončena i pro platby.

Žádosti členů VP a jejich vyřízení, které byly v průběhu kontroly předloženy, byly vyřízeny v souladu s čl. 15-21 citovaného nařízení.

Kontrolující vyhodnotili zjištěný stav tak, že kontrolovaná osoba **neporušila** povinnost stanovenou v čl. 15-21 nařízení (EU) 2016/679, tedy že poskytuje subjektům údajů právo na přístup k osobním údajům.

Kontrolní zjištění č. 8:

Kontrolující rovněž zjišťovali podle čl. 28 nařízení (EU) 2016/679, kdo ve společnosti zpracovává osobní údaje, tj. zda kontrolovaná osoba využívá služeb zpracovatele a zda má uzavřenu příslušnou smlouvu, pokud mu zpracovatele nestanoví konkrétní zákon.

Kontrolou bylo zjištěno, že společnost jako správce zpřístupňuje osobní údaje členů VP zpracovatelům.

K předávání osobních údajů zpracovatelům dochází na základě smluv, které byly kontrolujícím předloženy.

Po zhodnocení obsahu předložených smluv proto kontrolující konstatují, že spolupráce správce a zpracovatele je nastavena způsobem, který odpovídá požadavkům čl. 28 odst. 2 a 3 nařízení (EU) 2016/679, čímž je dán i předpoklad k závěru, že **nedochází k porušení** základní povinnosti vyjádřené v odst. 1 citovaného nařízení.

Kontrolující proto vyhodnotili zjištěný stav tak, že společnost **neporušila** povinnost stanovenou v čl. 28 nařízení (EU) 2016/679.

Kontrolní zjištění č. 9:

Kontrolující dále ověřili plnění povinnosti, která společnosti vyplývá z čl. 30 odst. 1 nařízení (EU) 2016/679, tj. povinnost vést záznamy o činnostech zpracování.

Společnost předložila záznamy činnostech o zpracování, které jsou vedeny v písemné i v elektronické podobě, jejichž obsahem jsou následující skutečnosti:

- název a kontaktní údaje správce;
- jméno a kontaktní údaje pověřence pro ochranu osobních údajů;
- aktivita v rámci zpracování;
- subjekt údajů;
- kategorie osobních údajů;
- původce údajů (zdroj);
- účel zpracování;
- právní titul;
- jak jsou osobní údaje získávány;
- doba zpracování (lhůta pro výmaz);
- lomu jsou osobní údaje předávány (kategorie příjemců (zpracovatel/třetí strana) a titul předávání (smlouva/zákon));
- automatizované rozhodování;
- technická a organizační opatření. (podklad č. 5.3.)

Kontrolou bylo zjištěno, že společnost v pozici správce zpracovává záznamy o činnostech zpracování, které obsahují veškeré informace uvedené v čl. 30 odst. 1 písm. a) - g) nařízení (EU) 2016/679 (podklad č. 5.3.).

S ohledem na uvedené kontrolující konstatují, že společnost povinnost stanovenou v čl. 30 odst. 1 nařízení (EU) 2016/679 **neporušila**.

Kontrolní zjištění č. 10:

Kontrolující dále s ohledem na předmět kontroly hodnotili, zda a do jaké míry společnost plní povinnosti týkající se zabezpečení osobních údajů v souvislosti s VP, jak je jeho povinností podle čl. 32 nařízení (EU) 2016/679.

Soulad s právními předpisy, smluvními a jinými požadavky, ochranu dat a obchodní tajemství, prevenci zneužití výpočetní techniky a shodu s bezpečnostními politikami ověřuje společnost průběžně, zejména prostřednictvím následujících činností:

- pravidelné kontinuální činnosti:
  - kontrola správy evidencí;
  - identifikace nových zpracování;
  - školení nových zaměstnanců (doloženo)
  - ve spolupráci s HR oddělením;
  - zajištění právního souladu (monitoring právních předpisů);
  - dohled nad informacemi podávanými subjektům;
  - správa zpracovatelských smluv;
  - reakce na uplatněná práva subjektů údajů;
- pravidelné činnosti:
  - organizace pravidelného školení zaměstnanců (doloženo);
  - interní kontroly plnění povinností:
    - o oblast ochrany osobních údajů;
    - o oblast kybernetické bezpečnosti;
- nepravidelné činnosti:
  - posouzení vlivu na ochranu osobních údajů při nových zpracováních nebo jejich zásadní změně;
  - jednání vůči dozorovému úřadu;
  - vyhodnocování, zpracování a případné hlášení incidentů.

Dodržování povinností v oblasti zpracovávání a ochrany osobních údajů jsou oprávněni kontrolovat přímí nadřízení zaměstnance odpovědného za danou část zpracování osobních údajů, pověřený zástupce společníka či jím pověřená osoba a pověřenec pro ochranu osobních údajů.

Pro zpracování osobních údajů v rámci VP jsou používány elektronické databáze. Zabezpečení přístupů do IS je ve výlučné kompetenci pověřeného administrátora systému, včetně správy uživatelů a jejich přístupových oprávnění, což je zajištěno i technickými prostředky, přiřazením systémové role pro správu uživatelských oprávnění výlučně pověřenému pracovníkovi. Přístupové role jsou rozděleny na tři úrovně: administrátor, editor a čtenář.

Kontrolovaná osoba má vypracovanou řadu interních předpisů vztahujících se k zabezpečení osobních údajů, které byly v rámci kontroly předloženy.

V souvislosti s přijatými a realizovanými opatřeními společnost:

- předložila přehled záznamů přístupů pověřených zaměstnanců společnosti do elektronických databází. Z přehledu jsou patrné datum a čas přístupu, ID zákazníka, popis prováděné činnosti, dále ID, jméno a příjmení pověřeného zaměstnance a též identifikace účtu a uvedených databází. Tito zaměstnanci mohou na základě svých uživatelských oprávnění provádět v databázích operace na bázi individuálního člena VP. Uvedeným zaměstnancům, tedy pracovníkům reklamací, informací, dozoru pokladen, a uživateli vykonávajícímu u společnosti pracovní pozici operations specialista, je přístup k údajům konkrétního zákazníka umožněn na

základě identifikace dotčeného zákazníka pomocí jeho identifikačních údajů (bez takové identifikace nemá zaměstnanec, který řeší požadavky zákazníka, k osobním údajům přístup; operations specialista je navíc oprávněn do databází vstupovat též z titulu správy VP).

- doložila ke každé dotčené pracovní pozici její popis a dále potvrzení o školení/kontrolním testování z oblasti zpracování a ochrany osobních údajů dotčených zaměstnanců. K problematice školení sdělila, že v průběhu roku 2020 bylo plánováno přeškolení zaměstnanců společnosti v oblasti zpracování a ochrany osobních údajů. Plánované přeškolení bylo však realizováno pouze u zaměstnanců pracujících v ústředí společnosti, kteří mají k dispozici vlastní pracovní počítač. U zaměstnanců pracujících v objektech jednotlivých provozoven (hypermarketů) se však v roce 2020 plánované přeškolení neuskutečnilo, a to z důvodu pandemie onemocnění COVID-19. Přeškolení bude u zaměstnanců jednotlivých provozoven plošně realizováno, jakmile to pandemická situace a s ní spojená opatření dovolí.
- doložila vzor pracovní smlouvy, který obsahuje doložku o mlčenlivosti (pracovní smlouvy zaměstnanců takovou doložku standardně obsahují).
- ověřování identit uživatelů: ověřování identit uživatelů pro přístup k databázi osobních údajů, je řízeno vysoce zabezpečeným autentizačním mechanismem oAuth; autentizační služba poskytuje možnost ověření identity uživatele a jeho následnou autorizaci; detailní popis je obsažen v dokumentech Autentizace zákazníka (Uživatelská dokumentace) a Autentizace zákazníka (Technická dokumentace).
- přístupová oprávnění jsou řízena systémem Microsoft Active Directory implementovaným v rámci společnosti; uživatelé I. jsou v Active Directory začleněni do zvláštní security group;
- žádosti o zařazení uživatele do security group jsou transparentně a auditovatelně řízeny přes interní Service Desk;
- na úrovni společnosti byla přijata interní politika access managementu, která tvoří dokument Access management policy CZ .
- detekci, sběr a vyhodnocování kybernetických bezpečnostních událostí: potenciální výskyt případů bezpečnostních událostí je společností pravidelně a nepřetržitě kontrolován; za tímto účelem zavedla společnost odpovídající organizační a technické mechanismy; v případě, že zaměstnanec či jiná osoba zjistí, že došlo k případu bezpečnostní události a osobní údaje zpracovávané společnosti byly, jsou nebo mohou být v ohrožení, neprodleně o tom informuje svého nadřízeného nebo pověřence pro ochranu osobních údajů;
- aplikační bezpečnost: za účelem zajištění aplikační bezpečnosti jsou implementovány interní politiky a nařízení za účelem využívání moderních průmyslových standardů pro návrh aplikační architektury, datových integrací, bezpečných uživatelských rozhraní, zabezpečení přístupů a bezpečnostního monitoringu; interní politiky a nařízení jsou aktualizovány a modernizovány na pravidelné bázi.

V rámci zabezpečení osobních údajů, které společnost zpracovává, byla zavedena a přijata vhodná opatření pro zajištění úrovně zabezpečení odpovídající danému riziku.

Na základě výše uvedených skutečností dospěli kontrolující k závěru, že kontrolovaná osoba **neporušila** povinnosti dle čl. 32 nařízení (EU) 2016/679.

Kontrolní zjištění č. 11:

V souladu s ustanovením čl. 37 nařízení (EU) 2016/679, tj. povinnost správce jmenovat pověřence pro ochranu osobních údajů a tuto skutečnost oznámit Úřadu, bylo společností dne 30. ledna 2019 řádně oznámeno jmenování pověřence pro ochranu osobních údajů (podklad č. 18.1.).

V interní směrnici *Zpracování a ochrana osobních údajů* je v bodě 7 *Pověřenec pro ochranu osobních údajů* ustanovena funkce pověřence, uvedeny možné způsoby kontaktování této osoby a stručný popis jeho činností. (podklad č. 18.1.)

Jak vyplynulo ze zjištění kontrolujících pověřenec plní své povinnosti v souladu s nařízením (EU) 2016/679. (podklad č. 10.27.)

Kontrolující proto vyhodnotili zjištěný stav tak, že společnost jako správce **neporušila** povinnost stanovenou v čl. 37 nařízení (EU) 2016/679.

IV. Poučení o opravném prostředku:

Proti kontrolnímu zjištění uvedenému 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

Mgr. et Mgr. Božena Čajková	pověřená zaměstnankyně Úřadu	(podepsáno elektronicky) podpis
Bc. Hana Imiolková	pověřená zaměstnankyně Úřadu	(podepsáno elektronicky) podpis
Mgr. Zuzana Jeřábková	pověřená zaměstnankyně Úřadu	(podepsáno

elektronicky)

podpis