Úkol č.1
Internetový obchod se širokým sortimentem sportovního vybavení a oblečení provádí na základě vlastního monitoringu objednávek zákazníků jejich přiřazování do skupin podle toho, jaké sportovní zboží nejčastěji nakupují pro zasílání nabídek a případné poskytování věrnostních slev. Toto třídění zákazníků provádí ručně několik pracovníků marketingového oddělení, kteří zároveň zasílají na e-mailové adresy zákazníků odpovídající nabídky nového sortimentu zboží.

Posuďte, zda se jedná o profilování zákazníků. Jedná se v tomto případě současně o automatizované rozhodování? Mají subjekty údajů – zákazníci v tomto případě nárok na uplatnění svých práv podle čl.22, odst.1 Nařízení?

Odpověď:
O profilování se sice jedná, ale nejedná se o automatizované individuální rozhodování. Hodnocení je prováděno ručně jednotlivými pracovníky správce bez právních nebo obdobných významných účinků na zákazníky - SÚ. Takové zpracování z pohledu správce nepodléhá úpravě v čl. 22 Nařízení a lze jej provádět na základě obecných právních titulů podle čl. 6 Nařízení

Úkol č.3
Zaměstnavatel s cca 80 zaměstnanci provádí následující zpracování OÚ:

- personální agendu stávajících zaměstnanců v rámci vlastního personálního oddělení
- mzdovou agendu prostřednictvím externí účetní firmy
- předávání některých OÚ zaměstnanců zdravotní pojišťovně a ČSSZ
- kontrolu docházky prostřednictvím čipových karet s dobou uložení na zabezpečeném samostatném zařízení 2 měsíce
- monitoring vjezdu do areálu prostřednictvím 1 kamery bez záznamu zvuku
- monitoring vstupu do administrativní budovy prostřednictvím 1 kamery se záznamem zvuku se současnou evidencí návštěv prostřednictvím jejich zápisu do elektronické návštěvní knihy s archivací 1 rok
- monitoring uzavřeného areálu, který je ve vlastnictví zaměstnavatele, celkem 4 kamerami bez záznamu zvuku

Zaměstnavatel současně využívá služeb personální agentury ohledně náboru nových zaměstnanců. Personální agentura dle požadavků zaměstnavatele předává vybrané osobní údaje uchazečů o zaměstnání, které před tím shromáždila, přičemž konečný výběr uchazečů provádí sám zaměstnavatel prostřednictvím vlastního personálního oddělení.

Proveďte posouzení pravděpodobné výše rizika u jednotlivých zpracování OÚ a navrhněte, jaké kroky by měl zaměstnavatel jako správce OÚ učinit u jednotlivých zpracování OÚ (způsoby zabezpečení, smluvní vztahy, organizační opatření apod.). Na základě jakých právních titulů bude moci provádět jednotlivá zpracování OÚ? Zpracovává zaměstnavatel zvláštní kategorie OÚ a pokud ano, jaký právní titul bude potřeba k tomu, aby nedošlo k porušení souladu s Nařízením? Bude u některých prováděných zpracování OÚ potřeba zpracovat posouzení vlivu na ochranu OÚ?

Odpověď:

Personální agenda stávajících zaměstnanců v rámci vlastního personálního oddělení
Riziko: standardní
Právní titul zpracování: splnění právní povinnosti, oprávněný zájem správce,
Kroky z pohledu DPO: pseudonymizace OÚ, doporučení konkrétního určení účelů zpracování OÚ, kontrola určení odpovědných osob a konkrétních zpracovatelů – zaměstnanců správce, doporučit jasné

stanovení doby uložení OÚ (např. *„po dobu trvání pracovního poměru“*, *„3 roky po skončení pracovního poměru“* atd.), minimalizace OÚ bývalých zaměstnanců pro případ budoucího určení či výkon právních nároků správce vůči SÚ, provedení balančního testu na oprávněný zájem správce

Mzdová agenda prostřednictvím externí účetní firmy
Riziko: standardní
Právní titul zpracování: splnění pracovní smlouvy (povinnost vyplácet mzdu), splnění právní povinnosti
Kroky z pohledu DPO: POVINNOST SPRÁVCE uzavřít smlouvu se zpracovatelem s veškerými náležitostmi (účel zpracování, způsob předávání dat, rozsah předávaných OÚ, odpovědné osoby a konkrétní osoby, které budou zpracování provádět, povinnost mlčenlivosti, zákaz či dovolení zapojení dalšího zpracovatele - !!nutný souhlas správce!! atd.), pseudonymizace OÚ, doporučení způsobu archivace, způsobu předávání OÚ ke zpracování a způsobu předávání zpracovaných údajů

Předávání některých OÚ zaměstnanců zdravotní pojišťovně a ČSSZ
Riziko: nízké
Právní titul zpracování: splnění právní povinnosti (Zákon o veřejném zdrav. pojištění, Zákon o pojistném na sociální zabezpečení…..)
Kroky z pohledu DPO: kontrola určení konkrétního zaměstnance (pracovní náplň) správce k předávání těchto OÚ

Kontrola docházky prostřednictvím čipových karet s dobou uložení na zabezpečeném samostatném zařízení 2 měsíce
Riziko: standardní
Právní titul zpracování: splnění právní povinnosti (evidence docházky), oprávněný zájem správce
Kroky z pohledu DPO: zavedení pseudonymizace, kontrola určení odpovědné osoby za správu technického zařízení, nastavení a kontrola výmazu OÚ ve stanoveném časovém režimu, jak je řešena deaktivace karty v případě ztráty

Monitoring vjezdu do areálu prostřednictvím 1 kamery bez záznamu zvuku
Riziko: nízké až standardní
Právní titul zpracování: oprávněný zájem správce
Kroky z pohledu DPO: provedení balančního testu, informace o tom, že konkrétní prostor je monitorován a za jakým účelem, kontrola určení odpovědné osoby za provoz a správu technického zařízení, doporučení stanovení doby uložení záznamů a kontroly výmazu

Monitoring vstupu do administrativní budovy prostřednictvím 1 kamery se záznamem zvuku se současnou evidencí návštěv prostřednictvím jejich zápisu do elektronické návštěvní knihy s archivací 1 rok
Riziko: standardní
Právní titul zpracování: oprávněný zájem správce
Kroky z pohledu DPO: provedení balančního testu, informace o tom, že konkrétní prostor je monitorován a za jakým účelem, kontrola určení odpovědné osoby za provoz a správu technického zařízení, posouzení nezbytnosti záznamu zvuku, posouzení nezbytnosti poněkud delší doby uložení OÚ, posouzení určení správce, které údaje se budou zapisovat do návštěvní knihy – doporučení: jméno + firma nebo soukromě v kombinaci s č. OP (jedno či druhé), zda je prováděno poučení osob, které budou zapisovat do knihy návštěv a jakým způsobem je prokazováno

Monitoring uzavřeného areálu, který je ve vlastnictví zaměstnavatele, celkem 4 kamerami bez záznamu zvuku

Riziko: nízké

Právní titul zpracování: oprávněný zájem správce

Kroky z pohledu DPO: provedení balančního testu, informace o tom, že konkrétní prostor je monitorován a za jakým účelem, posouzení nezbytnosti takového počtu kamer k monitorování areálu, kontrola určení odpovědné osoby za provoz a správu technického zařízení, doporučit stanovení max. doby uložení záznamů a zajištění jejich výmazu

Nábor nových zaměstnanců přes personální agenturu

Riziko: nízké

- **v případě, že předávání OÚ uchazečů o zaměstnání bude probíhat přes zabezpečené úložiště správce, ke kterému bude mít přístup určený pracovník správce a určený pracovník personální agentury prostřednictvím např. logovacího klíče. Údaje mohou být navíc pseudonymizované**

Riziko: vysoké

- **v případě, že předávání OÚ uchazečů o zaměstnání bude probíhat prostřednictvím e-mailové komunikace mezi správcem a pracovní agenturou**

Právní titul zpracování: pokud se jedná o uchazeče o zaměstnání, tak je potřeba jeho souhlas se zpracováním OÚ, neboť správce těžko najde jiný právní důvod pro zpracování. Předpokládejme ovšem, že uchazeč jako SÚ dal souhlas se zpracováním svých OÚ pro potřeby zajištění pracovního místa personální agentuře, vč. jejich předání konkrétní organizaci, která poptává pracovní místa.

Kroky z pohledu DPO: kontrola určení osob, které budou mít přístup do sdíleného úložiště a které budou s předanými OÚ dále pracovat v organizaci správce, zajištění výmazu OÚ uchazečů, kteří nebyli vybráni a kteří nedali případný souhlas s uložením svých OÚ u správce pro případ budoucí poptávky pracovních míst, doporučení určení max. doby pro uložení takových OÚ a zajištění jejich následného výmazu

Ze zadání nevyplývá, že by zaměstnavatel – správce zpracovával zvláštní kategorie OÚ (citlivé údaje)

Dle zadaného rozsahu zpracování OÚ nebude s největší pravděpodobností nutné zpracovat posouzení vlivu na ochranu práv SÚ