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 (či spíše scoring) se sice jedná, ale nejedná se o automatizované individuální rozhodování, takže taková činnost nebude v rozporu s GDPR. Hodnocení je prováděno ručně jednotlivými pracovníky správce bez právních nebo obdobných negativních 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.2

Výrobce automobilů detekoval, že v určité sérii modelové řady se vyskytla kritická vada – možná samoaktivace airbagu spolujezdce. Tato výrobní série vozidel byla dodána do konkrétního státu před cca 2 měsíci. Za tímto účelem hodlá kontaktovat správce centrálního registru vozidel, aby mu předal jmenný seznam jejich vlastníků s kontaktními údaji, aby je mohl informovat o možnostech bezplatného odstranění této poruchy.

Posuďte podle čl.6 Nařízení z pozice případného DPO správce registru, zda je tento oprávněn předat požadované údaje výrobci vozidel a odůvodnit, podle jakého právního titulu byste případně na základě konzultace doporučili jejich předání k dalšímu zpracování (jinému účelu zpracování než za kterým byly původně shromážděny) výrobci automobilů.

Odpověď:

Správce registru je oprávněn předat požadované OÚ výrobci vozidel. Tyto OÚ je možné předat na základě Právního titulu dle čl. 6, odst. 4, písm. d) Nařízení. Jedná se sice o zpracování OÚ k jinému účelu než byly původně shromážděny, nicméně možné důsledky takového zamýšleného zpracování OÚ nelze posuzovat pouze z pohledu, zda budou mít pro SÚ pravděpodobně negativní účinky, ale také z pohledu případných pozitivních důsledků. V tomto případě se zcela zjevně jedná o provedení opatření – výměnu vadné součástky airbagu, která může zabránit nehodě. Na tento případ je tedy možné uplatnit právní titul, že takové zpracování je nezbytné pro ochranu životně důležitých zájmů SÚ nebo jiné fyzické osoby podle čl. 6, odst. 1, písm. d) 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: nízké - za předpokladu používání zabezpečeného prostředí a zpracování pouze pověřenými pracovníky !!! zmínit rostoucí riziko ve vztahu k technickým a organizačním opatřením !!!

Právní titul zpracování: splnění právní povinnosti, oprávněný zájem správce,

Kroky z pohledu DPO: pseudonymizace OÚ, doporučení stanovení konkrétního určení účelů zpracování OÚ jednotlivými zpracovateli, kontrola určení odpovědných osob a konkrétních zpracovatelů – zaměstnanců správce, doporučit jasné stanovení doby uložení OÚ (např. *„po dobu trvání pracovního poměru“, „1 rok po skončení pracovního poměru“, „po dobu předpisem stanovené archivace“* atd.), minimalizace OÚ bývalých zaměstnanců pro případ budoucího určení či výkon právních nároků správce vůči SÚ, případně provedení balančního testu na oprávněný zájem správce.

Doporučení: zvážit zpracování posouzení vlivu na ochranu OÚ – DPIA, záznamy o činnostech zpracování dle čl. 30

!!! Pozor na zpracovávání rodných čísel, pokud pro to neexistuje právní povinnost, pak lze pouze se souhlasem nositele rodného čísla – SÚ. – viz § 13c zákona č. 133/2000 Sb, o evidenci obyvatel a rodných číslech. Podobně u pořizování kopií občanských průkazů – viz § 15a zákona č. 328/1999 Sb., zákon o občanských průkazech !!!

==========

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

§13c, odst.1 – *Rodná čísla lze využívat jen*

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

b) stanoví-li tak zvláštní zákon, nebo

c) se souhlasem nositele rodného čísla nebo jeho zákonného zástupce.

Zákon č. 328/1999 Sb., o občanských průkazech:

§15a, odst.2

„Je zakázáno pořizovat jakýmikoliv prostředky kopie občanského průkazu bez prokazatelného souhlasu[1]) občana, kterému byl občanský průkaz vydán, pokud zvláštní zákon nebo mezinárodní smlouva, kterou je Česká republika vázána, nestanoví jinak“.

[1]) podle §5 zákona č. 101/2000 Sb., o ochraně OÚ

==========

Mzdová agenda prostřednictvím externí účetní firmy

Riziko: nízké – při přijetí dostatečných technicko – organizačních opatření jak na straně správce tak na straně případného zpracovatele. !!! Pozor na způsob předávání podkladů ke zpracování externímu zpracovateli – v žádném případě jako prostá příloha e-mailu (zip + heslo, šifrování např. přes Outlook) !!!

Právní titul zpracování: splnění pracovní smlouvy (povinnost vyplácet mzdu) v kombinaci se splněním právní povinnosti (hlášení, přehledy, evidence..)

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. Pro případ ukončení zpracovatelské smlouvy jasně stanovit způsob zpětného předání veškerých OÚ a evidencí správci a zajištění likvidace OÚ na straně zpracovatele pod kontrolou správce.

Předávání některých OÚ zaměstnanců zdravotní pojišťovně a ČSSZ

Riziko: nízké - (datové schránky, poštovní přeprava (listovní tajemství, osobní předání na podatelně)

Právní titul zpracování: splnění právní povinnosti (Zákon o veřejném zdrav. pojištění, Zákon o pojistném na sociální zabezpečení, Zákon o důchodovém pojištění…..)

Kroky z pohledu DPO: kontrola určení konkrétního zaměstnance (pracovní náplň) správce k předávání těchto OÚ, v případě externího zpracovatele plná moc

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 např. prostřednictvím osobních čísel, kontrola určení odpovědné osoby za správu technického zařízení pro evidenci, 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 – v rámci možností zabírat co nejmenší část veřejných prostor či prostranství

Právní titul zpracování: oprávněný zájem správce

Kroky z pohledu DPO: provedení balančního testu, zveřejnění 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, vedení dokumentace o provozu technického zařízení a provedených výmazech záznamů

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: střední

Právní titul zpracování: oprávněný zájem správce

Kroky z pohledu DPO: kontrola 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, vedení dokumentace o provozu technického zařízení a provedených výmazech záznamů, posouzení nezbytnosti záznamu zvuku, posouzení nezbytnosti poněkud delší doby uložení OÚ, které údaje se budou zapisovat do návštěvní knihy – doporučení: jméno a příjmení + firma nebo soukromě v kombinaci s č. OP (jedno či druhé), zda je prováděno poučení osob, které budou zapisovat do knihy návštěv a vedení dokumentace k poučení

Doporučení: podle rozsahu posouzení vlivu na ochranu OÚ, záznam o činnostech zpracování podle čl. 30 Nařízení

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

Riziko: nízké - střední

Právní titul zpracování: oprávněný zájem správce

Kroky z pohledu DPO: kontrola 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, vedení dokumentace o provozu technického zařízení a provedených výmazech záznamů

Doporučení: dle rozsahu posouzení vlivu na ochranu OÚ, záznam o činnostech zpracování podle čl. 30 Nařízení

Nábor nových zaměstnanců přes personální agenturu

Riziko: nízké

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

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

Kroky z pohledu DPO: průběžná kontrola určení osob, které budou mít přístup do sdíleného úložiště a které budou s předanými OÚ dále pracovat v organizaci správce, stanovení osob,

kterým budou v rámci organizace OÚ uchazeče předávány k případnému rozhodnutí, 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