Metodická doporučení pro kluby Autoklubu ČR, týkající se zabezpečení osobních údajů v oblasti IT

s cílem zajistit soulad s nařízením 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, „GDPR“).

1. Úvod

Součástí GDPR jsou i povinnosti správců a zpracovatelů při využívání informačních technologií. Tyto povinnosti jsou vyjádřeny především v článku 32 GDPR "Zabezpečení zpracování". Podle tohoto článku jsou správce i zpracovatel povinni *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, provést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku.*

GDPR tedy nestanoví zcela přesný návod, jakým způsobem je třeba osobní data zabezpečit, ale obecnou povinnost takové zabezpečení zajistit. Podstatná je však jasně proklamovaná zásada přiměřenosti, a to jak vzhledem k náročnosti zabezpečení, tak i "citlivosti" zpracovávaných dat. Následující metodická doporučení jsou tedy uvedena s přihlédnutím k výše uvedenému.

2. Zabezpečení HW

Data v IT systémech jsou lokálně uložena na počítači, notebooku, telefonu či různých paměťových médiích. S přihlédnutím k zásadě přiměřenosti je třeba přijmout alespoň základní opatření, aby nedošlo k jejich ztrátě nebo neoprávněnému přístupu. To představuje následující soubor opatření:

2.1. Pokud je to možné, opatření HW heslem či PINem;

2.2. Pokud je to možné, zašifrování HDD notebooku či počítače, aby v případě ztráty či odcizení nebylo možno data přečíst[1];

[1] zde je třeba připomenout, že ztráta notebooku či telefonu patří z pohledu zneužití osobních údajů k jednomu z nejčastějších rizik, se kterým je třeba počítat

2.3. Zajištění přiměřených opatření, aby k danému HW neměl přístup nikdo jiný, než osoba oprávněná nakládat s osobními daty (pokud nejsou uložena ve zvlášť zajištěné databázi)[2];

2.4. Fyzické zabezpečení k HW (např. uložení paměťových sestav, HDD apod. v uzamykatelné skříňce).

3. Zabezpečení SW nástrojů pro zpracování dat

3.1. Důsledná ochrana všech programů alespoň pomocí hesla (pokud to jde, tak i dvoufaktorovou autentizací);

3.2. Instalace antiviru, pravidelná kontrola a udržování antivirové databáze;

3.3. Pravidelná aktualizace operačního systému, internetových prohlížečů a dalších aplikací (Acrobat Reader, Java, Flash Player atd.);

3.4. Pravidelné zálohování důležitých dat (součástí pravidel GDPR jsou i opatření proti ztrátě dat);

3.5. Využívání uživatelských účtů (aneb pod jedním účtem a heslem by nikdy k aplikaci neměly přistupovat různé osoby);

3.6. Pokud je to možné, zajistit, aby k údajům měly přístup jen osoby, které jsou k tomu pověřeny;

3.7. Pokud je počítač připojen k síti, vždy používat firewall (základní firewall je součástí operačního systému);

3.8. Pokud je umožněn vzdálený přístup přes internet (např. sdílený disk, NAS, intranet apod.) vždy používat zabezpečené připojení pomocí SSL certifikátu (Https).

4. Stanovení základních bezpečnostních pravidel

Za účelem zajištění dodržování uvedených pravidel by každý klub měl stanovit závazná bezpečnostní pravidla pro nakládání s IT prostředky. K dodržování těchto pravidel by měli být zavázáni všichni uživatelé, kteří se na zpracování osobních údajů podílejí, a dále i ti, kteří mají přístup k HW prostředkům, kde jsou osobní údaje uloženy.

Kromě výše uvedených zásad by měl klub zajistit:

4.1. stanovení politiky přístupových hesel;

---

[2] velkým problémem může být uchovávání dat na počítači, nad kterým nemá uživatel plnou kontrolu (např. počítač, který byl zapůjčen zaměstnavatelem)

4.1.1. používat pouze bezpečná hesla, tzn. hesla by neměla být snadno odhadnutelná, měla by obsahovat alespoň jedno velké písmeno a číslici a mít dostatečnou délku;

4.1.2. hesla by měla být pravidelně měněna;

4.1.3. neměla by být používána stejná hesla pro přístup k různým systémům;

4.1.4. hesla nesdělovat třetím osobám ani si je nepoznamenávat na nevhodná místa (zápisník u počítače, apod.).

4.2. uživatelé by měli postupovat tak, aby jimi používaná zařízení nebyla napadena škodlivým softwarem, který může způsobit únik osobních údajů, zejména:

4.2.1. neotevírat přílohy e-mailů, které nepochází z důvěryhodných zdrojů;

4.2.2. nenavštěvovat internetové stránky s potenciálně nebezpečným softwarem (zejména stránky umožňující bezplatně stahovat autorskoprávně chráněné filmy či hudbu a pornografické stránky, stránky, na které odkazuje reklama slibující snadný výdělek v nezvyklé výši, apod.);

4.2.3. provádět pravidelné aktualizace softwaru v zařízeních.

4.3. nezanechávat služební zařízení a dokumenty obsahující osobní údaje bez dozoru, pokud nejsou řádně uzamčeny a chráněny (zámkem, šifrováním, apod.);

4.4. osobní údaje ukládat na přenosná zařízení (např. USB disky) pouze v šifrované podobě.

Je třeba upozornit, že k efektivnímu dodržování pravidel je rovněž nutné zajistit v přiměřeném rozsahu i jejich kontrolu.

5. Další zpracovatelé

V oblasti IT dochází velmi často k využití dalších zpracovatelů. Vzhledem k tomu, že zpracování osobních údajů je i jejich pouhé uložení, takovými zpracovateli mohou být např. poskytovatelé cloudových služeb (záloha telefonu), poskytovatelé různých SW jako služby, hostingová centra, kde jsou uloženy internetové stránky, sociální sítě apod. Základní povinností je přitom ubezpečit se, že s daty je u těchto zpracovatelů nakládáno v souladu s GDPR. U velkých společností je toto zpravidla součástí aktualizovaných smluvních podmínek. Ujistěte se proto, že i zpracovatelé, které jste vy zapojili do zpracování, nakládají s daty v souladu s GDPR.

V případě, že využíváte nějaký speciální SW (např. účetní program, personální program apod.), je vhodné s dodavatelem SW zajistit dodatek ke smlouvě, ve kterém dodavatel bude garantovat, že program dodržuje příslušné bezpečnostní standardy.