Právní audit GDPR dokumentace

Výsledek: PASS [(s výhradami)]

Odůvodnění

Předložený soubor dokumentace (dokumenty 1 až 5) byl podroben hloubkovému právnímu a compliance auditu se zaměřením na soulad s legislativním rámcem platným v České republice a Evropské unii k prosinci 2025. Auditovaná dokumentace představuje **systémový základ**, který po doplnění specifických procesních parametrů a proměnných bude plně způsobilý demonstrovat soulad s Obecným nařízením o ochraně osobních údajů (GDPR).

Dokumentace vykazuje vysokou míru vyspělosti a reflektuje nejen statické požadavky nařízení, ale i dynamický vývoj judikatury a rozhodovací praxe dozorových úřadů v letech 2023–2025. Zejména je nutné vyzdvihnout správnou reflexi transatlantických datových toků po stabilizaci rámce EU-US Data Privacy Framework a přesnou aplikaci novelizovaných retenčních lhůt v oblasti mzdové agendy.

Co je v pořádku:

- **Reflexe legislativních změn v retenci dat:** Dokumenty správně identifikují retenční lhůtu 45 let pro mzdové listy a údaje pro důchodové pojištění. Toto nastavení je v souladu s novelizovaným zněním § 35a odst. 4 písm. d) zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení, účinným od roku 2023.[1]
- **Legalizace mezinárodních přenosů:** Dokumentace správně opírá předávání dat do USA (Google, Mailchimp/Intuit) o rozhodnutí o přiměřenosti pro *EU-US Data Privacy Framework* (DPF). Audit potvrdil, že jak Google LLC, tak Intuit Inc. (mateřská společnost The Rocket Science Group) jsou k prosinci 2025 aktivními a certifikovanými účastníky tohoto rámce.[4] Tím je splněna podmínka čl. 45 GDPR bez nutnosti složitého sjednávání Standardních smluvních doložek (SCC) a doplňkových opatření.
- **Struktura informační povinnosti (Transparency Principle):** Rozdělení na detailní „Zásady“ a stručný „Informační list“ (One-pager) odpovídá doporučením EDPB pro transparentnost dle čl. 12 GDPR, kdy je subjektu údajů informace dávkována srozumitelným způsobem (vrstvený přístup).[4]
- **Procesní uchopení práv subjektů:** Šablony obsahují kompletní katalog práv (čl. 15–22 GDPR) a správně definují kanály pro jejich uplatnění, včetně explicitního uvedení kontaktu na Úřad pro ochranu osobních údajů (ÚOOÚ).[4]

---

1. Komplexní analýza legislativního a judikatorního

kontextu (2025)

Pro pochopení kontextu, ve kterém bude tato dokumentace aplikována, je nezbytné analyzovat širší právní prostředí roku 2025. GDPR již není izolovaným předpisem, ale součástí komplexního ekosystému digitální regulace EU, který zahrnuje Akt o datech (Data Act), Akt o umělé inteligenci (AI Act) a směrnici NIS2. Auditovaná dokumentace musí být hodnocena nejen z pohledu textu samotného nařízení, ale i z pohledu její interoperability s těmito normami.

1.1 Stabilizace transatlantických datových toků (Post-Schrems II éra)

Jedním z kritických bodů compliance v letech 2020–2023 byla nejistota ohledně legálnosti využívání amerických cloudových služeb (Google Analytics, Mailchimp atd.) po rozsudku *Schrems II*. V dokumentaci [4] je uveden jako právní základ pro přenos do USA „Rozhodnutí Evropské komise o přiměřenosti ochrany (Data Privacy Framework)“.

Tato formulace je v roce 2025 **zcela správná a klíčová**. Soudní dvůr Evropské unie (SDEU) v roce 2025 (ve věci *Philippe Latombe v. Evropská komise*) potvrdil platnost tohoto rámce a odmítl žalobu na neplatnost, čímž ukončil období právní nejistoty.[7] Soud potvrdil, že mechanismy nápravy v USA (Data Protection Review Court) poskytují občanům EU dostatečné záruky.

Dokumentace tak správně reflektuje, že pokud je příjemce v USA (zde Google a Intuit) certifikován v DPF, pohlíží se na přenos, jako by probíhal v rámci EHP (čl. 45 GDPR). To zásadně zjednodušuje administrativu správce, který nemusí provádět složitý *Transfer Impact Assessment* (TIA), jenž byl vyžadován v předchozích letech.

Důležitý detail: V dokumentaci [4] je u Mailchimpu správně uvedena mateřská společnost *Intuit Inc.* jako nositel certifikace DPF. Audit registrů DPF potvrdil, že *The Rocket Science Group LLC* (provozovatel Mailchimpu) je vedena jako "Covered Entity" pod certifikací Intuit Inc..[5] Tato přesnost v šabloně je známkou vysoké kvality přípravy podkladů.

1.2 Průnik GDPR a kybernetické bezpečnosti (NIS2/ZKB)

V roce 2025 nabyl v České republice plné účinnosti nový zákon o kybernetické bezpečnosti (implementující směrnici NIS2). Tento předpis dramaticky rozšiřuje okruh povinných subjektů (z původních stovek na tisíce firem), na které dopadají povinnosti hlášení incidentů.

Auditovaná *Směrnice pro řešení bezpečnostních incidentů* [4] pracuje s lhůtou 72 hodin pro ohlášení ÚOOÚ (dle čl. 33 GDPR). Zde však vzniká potenciální kolize pro subjekty, které spadají i pod regulaci NIS2. Tyto subjekty mají povinnost hlásit kybernetický incident (který je často i incidentem porušení zabezpečení osobních údajů) Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB), a to v režimu „včasného varování“ do **24 hodin**.[10]

Ačkoliv šablona splňuje požadavky GDPR, pro kompletní právní bezpečnost v roce 2025 by měla obsahovat tzv. "NIS2 check" – tedy procesní krok, kdy správce ověří, zda incident nepodléhá i hlášení NÚKIB. Pokud ano, lhůta 72 hodin pro ÚOOÚ je sice platná, ale procesně sekundární oproti 24hodinové lhůtě pro NÚKIB. Absence tohoto upozornění je hodnocena jako výhrada (viz sekce Výhrady).

1.3 Retence dat a specifika mzdové agendy

Oblast archivace a skartace je v dokumentaci zpracována s nadstandardní přesností. U mzdových listů je uvedena lhůta 45 let. Toto reflektuje změnu § 35a odst. 4 písm. d) zákona č. 582/1991 Sb., která reagovala na prodlužování věku odchodu do důchodu a potřebu delšího uchování podkladů pro ČSSZ.[2]

Mnoho starších vzorů stále operuje s lhůtou 30 let, což je v roce 2025 již chybné a vystavuje správce riziku pokuty nejen od ÚOOÚ (za porušení principu přesnosti), ale především od orgánů sociálního zabezpečení. Auditovaná dokumentace tento "chyták" české legislativy zvládla správně.

Zároveň je správně nastavena lhůta 10 let pro účetní doklady (faktury s DPH) dle § 35 zákona o DPH.[13] Rozlišení těchto lhůt v dokumentu *Zásady zpracování* [4] demonstruje soulad se zásadou omezení uložení (čl. 5 odst. 1 písm. e) GDPR).

---

2. Analýza Zásad zpracování a Informační povinnosti (Dokumenty 1 a 2)

Informační povinnost je základním pilířem transparentnosti. Audit zkoumal, zda šablony pokrývají všechny povinné body dle čl. 13 a 14 GDPR a zda jsou srozumitelné.

2.1 Identifikace správce a účelů

Dokumenty obsahují jasná pole pro identifikaci správce. Klíčovým pozitivem je strukturované propojení **Účel – Právní základ – Doba uložení**. Toto propojení je nezbytné pro splnění požadavku „fair processing“. Subjekt údajů musí vědět nejen *proč* jsou data zpracovávána, ale *na základě čeho* a *jak dlouho*.

2.2 Kategorizace příjemců

Dokumentace uvádí konkrétní kategorie příjemců (účetní, hosting, platební brána) a jmenuje klíčové zpracovatele (Google, Mailchimp). Ačkoliv GDPR v čl. 13 odst. 1 písm. e) vyžaduje uvedení „příjemců nebo kategorií příjemců“, v kontextu rozhodovací praxe ÚOOÚ a EDPB se doporučuje u hlavních zpracovatelů uvádět konkrétní názvy, zejména pokud dochází k přenosu

do třetích zemí. Šablona tento požadavek plní.

2.3 Analýza cookies a analytiky v roce 2025

Dokument [4] uvádí u "Analytiky webu" a "Personalizace" jako právní základ "Souhlas". To je v souladu s transpozicí směrnice ePrivacy do českého zákona o elektronických komunikacích (§ 89 odst. 3 ZEK), který vyžaduje režim **opt-in** pro všechny netechnické cookies.[15]

Zde však audit naráží na technickou nuanci. Šablona uvádí dobu uchování u analytiky 14 měsíců. Tato doba odpovídá standardnímu nastavení Google Analytics 4 (GA4). Je však nutné upozornit, že výchozí nastavení GA4 může být 2 měsíce, a správce musí aktivně změnit nastavení na 14 měsíců, aby text dokumentace odpovídal realitě.[17] Pokud by správce měl nastaveno 2 měsíce, ale informoval o 14, dochází k formálnímu nesouladu (byť ve prospěch subjektu údajů). Naopak, u verze GA4 360 může být retence až 50 měsíců.[18] Šablona je nastavena na nejčastější scénář (standardní GA4 s manuálním prodloužením na 14 měsíců), což je akceptovatelné, ale vyžaduje kontrolu nastavení nástroje.

---

3. Hodnocení Souhlasu a Právních základů (Dokument 3)

GDPR staví souhlas na roveň ostatním právním titulům, avšak v praxi je to nejkřehčí titul. Audit se zaměřil na kvalitu formulace souhlasu.

3.1 Dobrovolnost a granularita

Dokument [4] správně odděluje souhlasy pro různé účely ("Marketing/newsletter" vs. "Personalizace/profilování"). Tato granularita je nezbytná dle recitálu 43 a čl. 7 GDPR. Pokud by byl souhlas sloučen ("balíčkový souhlas"), byl by neplatný. Šablona tímto rizikem netrpí.

3.2 Odvolatelnost

Dokument jasně deklaruje, že souhlas lze kdykoli odvolat, a uvádí konkrétní způsoby (e-mail, odkaz v patičce, webový formulář). To naplňuje požadavek čl. 7 odst. 3 GDPR ("odvolání musí být stejně snadné jako poskytnutí").

3.3 Problematika "Soft Opt-in"

V dokumentaci se objevuje paušalizace marketingu pod "Souhlas". Je třeba upozornit, že pro stávající zákazníky lze využít tzv. zákaznickou výjimku (soft opt-in) dle § 7 odst. 3 zákona č. 480/2004 Sb., kdy je právním titulem Oprávněný zájem správce, nikoli Souhlas.19
Šablona dokumentu 3 je koncipována pro nové zájemce (opt-in). Pokud by správce tuto šablonu používal i pro své stávající zákazníky (např. nutil je znovu udělovat souhlas), zatěžoval

by se zbytečnou administrativou a riskoval by ztrátu části databáze. Audit doporučuje v dokumentu Zásady zpracování explicitněji rozlišit "Marketing pro zákazníky" (Oprávněný zájem) a "Marketing pro ostatní" (Souhlas), aby byla dokumentace plastičtější.

---

4. Záznamy o činnostech zpracování - RoPA (Dokument 4)

Dokumentace dle čl. 30 GDPR je "vstupenkou" do jakékoli kontroly ÚOOÚ.

4.1 Obsahová úplnost

Předložená tabulka [4] obsahuje všechny povinné sloupce dle čl. 30 odst. 1:

- Účel zpracování
- Kategorie subjektů a osobních údajů
- Kategorie příjemců
- Přenosy do třetích zemí
- Lhůty pro výmaz
- Popis bezpečnostních opatření

4.2 Bezpečnostní opatření

Popis technických a organizačních opatření (šifrování, řízení přístupu, zálohování) je v šabloně obecný, což je pro RoPA přípustné (čl. 30 požaduje "obecný popis"). Důležité je, aby realita ve firmě těmto deklaracím odpovídala. Zmínka o HTTPS/TLS a pravidelném zálohování je standardem, který ÚOOÚ očekává.

---

5. Bezpečnostní incidenty a Směrnice (Dokument 5)

Proces řízení incidentů je kritický pro minimalizaci škod a sankcí.

5.1 Procesní lhůty

Šablona [4] správně definuje lhůtu 72 hodin pro ohlášení dozorovému úřadu. Rozlišuje také mezi povinností "ohlásit úřadu" (všechna rizika kromě nepravděpodobných) a "oznámit subjektu" (jen vysoká rizika). Tato distinkce dle čl. 33 a 34 GDPR je klíčová pro zamezení "over-reporting" (zbytečného hlášení banalit), které by mohlo firmu poškodit reputačně.

5.2 Formulář a kanály hlášení

Dokument odkazuje na web ÚOOÚ a datovou schránku. Pro rok 2025 je relevantní, že ÚOOÚ upřednostňuje elektronická podání (datová schránka, e-podatelna). Šablona obsahuje

správné ID datové schránky ÚOOÚ (qkbaa2n).[4]

Výhrady/Nedostatky

Níže uvedená tabulka shrnuje oblasti, které vyžadují pozornost nebo úpravu pro dosažení plné compliance a optimalizaci procesů.

Problém	Závažnost	Popis a doporučení
Absence reflexe NIS2	**Střední**	Šablona pro incidenty neobsahuje vazbu na nový zákon o kybernetické bezpečnosti (NIS2). Pokud je správce "regulovaným subjektem" (což může být i větší e-shop, dopravce, výrobní firma), musí hlásit incidenty NÚKIB do 24 hodin. **Doporučení:** Doplnit do směrnice "rozcestník" ověřující, zda firma nespadá pod NIS2.
Marketing: Souhlas vs. Oprávněný zájem	**Střední**	Dokumentace paušálně řadí marketing pod "Souhlas". U stávajících zákazníků je to zbytečné a administrativně náročné (nutnost re-consent). **Doporučení:** V Zásadách rozdělit marketing na "Přímý marketing zákazníkům" (Oprávněný zájem) a "Newsletter pro ostatní" (Souhlas).
Specifikace doby u GA4	**Nízká**	Uvedená doba 14 měsíců u analytiky vyžaduje aktivní zásah v nastavení GA4 (default je 2 měsíce).

		Doporučení: Přidat do interních poznámek pokyn pro IT/Marketing k ověření nastavení v Google Analytics.
Biometrie v docházce	**Střední**	Pokud by "Zaměstnanecká agenda" zahrnovala docházku na otisk prstu, pouhý odkaz na "právní povinnost" nestačí (ÚOOÚ to často rozporuje). **Doporučení:** Pokud se používá biometrie, je nutné provést DPIA a ověřit nezbytnost (čl. 9 GDPR). V šabloně to explicitně chybí.

Verdikt

Předložená dokumentace představuje **velmi kvalitní a aktuální základ** pro řízení ochrany osobních údajů. Nejedná se o zastaralé vzory; dokumenty reagují na legislativní realitu let 2023–2025 (zejména v oblasti mzdové retence a transferů do USA).

Systém dokumentace **obstojí při kontrole ÚOOÚ**, za předpokladu, že:

1. Budou nahrazeny placeholdery reálnými údaji.
2. Klient si ověří, zda nespadá pod regulaci NIS2 (což by změnilo proces hlášení incidentů).
3. Technické nastavení nástrojů (GA4, Mailchimp) bude korespondovat s údaji v dokumentech (zejména retenční doby).

Doporučená oprava před nasazením:
V dokumentu Zásady zpracování a Záznamy o činnostech doporučuji explicitně rozdělit účel "Marketing" na dvě větve:

1. **Marketing vůči zákazníkům** -> Právní základ: **Oprávněný zájem** (čl. 6 odst. 1 písm. f) GDPR ve spojení s § 7 odst. 3 zákona č. 480/2004 Sb.).
2. **Marketing vůči ostatním (potenciálním klientům)** -> Právní základ: **Souhlas** (čl. 6 odst. 1 písm. a) GDPR).

Tato úprava lépe odráží realitu e-commerce a snižuje riziko ztráty kontaktů při zbytečném vyžadování souhlasu tam, kde to zákon nevyžaduje.

V ostatních aspektech je dokumentace **PASS**.

Komplexní analýza a odůvodnění auditu GDPR dokumentace

Následující část reportu poskytuje detailní vhled do právních úvah, judikatury a výkladové praxe, která vedla k výše uvedenému verdiktu. Tato analýza slouží pro hlubší pochopení souvislostí a jako manuál pro správnou implementaci šablon v praxi roku 2025.

1. Metodologický a legislativní rámec auditu (Stav 2025)

Audit byl proveden s vědomím, že GDPR v roce 2025 již není novinkou, ale zavedeným standardem, který je však neustále formován novými technologiemi a navazující legislativou.

1.1 Posun od formálního k materiálnímu souladu

V prvních letech po účinnosti GDPR (2018–2020) se kontroly ÚOOÚ často zaměřovaly na formální existenci dokumentů. V roce 2025 se těžiště přesouvá k materiálnímu souladu a accountability (odpovědnosti). Dozorové úřady již nezkoumají jen to, zda máte směrnici, ale zda procesy v ní popsané reálně fungují.
Proto je v auditu kladen důraz na provázanost dokumentů (např. zda lhůta v Zásadách odpovídá nastavení v softwaru). Předložené šablony tím, že obsahují konkrétní lhůty (14 měsíců, 45 let) a nikoli jen vágní fráze typu "po dobu nezbytně nutnou", nutí správce k zamyšlení nad realitou zpracování, což je pozitivní rys.

1.2 Interoperabilita s Digitálním balíčkem EU

Rok 2025 je rokem implementace a prvních kontrol v rámci nových digitálních předpisů EU. GDPR dokumentace nemůže existovat ve vakuu.

- **Data Act & AI Act:** Ačkoliv šablony explicitně nezmiňují umělou inteligenci, definice účelů jako "Personalizace obsahu a profilování" [4] vytváří prostor pro využití algoritmických systémů. Je klíčové, aby správce při nasazení AI nástrojů (např. pro scoring zákazníků) aktualizoval RoPA a Zásady o informace vyžadované AI Actem (transparentnost ohledně interakce s AI). Auditovaná dokumentace je v tomto směru "AI-ready", protože správně pracuje s pojmem profilování dle čl. 22 GDPR.
- **NIS2 (Zákon o kybernetické bezpečnosti):** Jak bylo zmíněno ve výhradách, toto je největší třecí plocha. Dokumentace se drží 72hodinové lhůty GDPR. Pro mnoho firem to bude stačit. Pro dodavatele v rámci dodavatelských řetězců regulovaných služeb to však může být nedostatečné. Audit upozorňuje na nutnost harmonizace procesu incident

managementu, aby vyhověl oběma režimům.

2. Hloubková analýza Zásad zpracování (Privacy Policy)

Dokument *Zásady zpracování* [4] je výkladní skříní správce. Jeho analýza odhalila několik klíčových silných stránek a nuancí.

2.1 Mzdová a personální agenda: Konec 30letého mýtu

V české praxi dlouho panoval úzus (podpořený starším zněním zákona), že mzdové listy se uchovávají 30 let. Novelizace zákona č. 582/1991 Sb., která proběhla zákonem č. 455/2022 Sb. s účinností od 1. 1. 2023, tuto lhůtu pro "mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění" prodloužila na 45 let.1
Tato změna reaguje na demografický vývoj a potřebu mít k dispozici data pro výpočet důchodů po delší dobu aktivního života občanů.

- **Auditní nález:** Šablona [4] uvádí "Zaměstnanecká agenda: 45 let". Toto je **správně**. Pokud by šablona obsahovala starých 30 let, jednalo by se o FAIL v oblasti zákonnosti zpracování (nedovolené zkrácení doby pro plnění právní povinnosti).

2.2 Transatlantické přenosy: Konec nejistoty

Vztah mezi EU a USA v oblasti dat byl dlouho turbulentní (zrušení Safe Harbor, zrušení Privacy Shield). Od července 2023, kdy Evropská komise přijala rozhodnutí o přiměřenosti pro *EU-US Data Privacy Framework* (DPF), a po jeho potvrzení Tribunálem EU v roce 2025 (zamítnutí žaloby Philippa Latomba), je situace stabilní.[7]

- **Auditní nález:** Šablona se odvolává na DPF u Google a Mailchimp. Toto je **nejbezpečnější a administrativně nejméně náročný způsob** legalizace přenosu. Alternativou by byly Standardní smluvní doložky (SCC) doplněné o Transfer Impact Assessment (TIA), což je pro běžného správce extrémně náročné. Využití DPF je tedy pragmatickou a právně konformní volbou.
- **Pozor:** Tato validita platí pouze, pokud jsou Google a Intuit na seznamu certifikovaných (Data Privacy Framework List). Audit potvrdil, že k datu auditu tam jsou. Správce by měl mít proces (např. roční kontrolu), kterým ověří, že tito dodavatelé z rámce nevypadli.

2.3 Analytika a doba uložení 14 měsíců

Uvedení lhůty 14 měsíců u Google Analytics [4] není náhodné. Jde o maximální dobu retence uživatelských dat (user-level data), kterou umožňuje bezplatná verze GA4 (u GA360 je to více).

- **Riziko:** Výchozí nastavení nové "property" v GA4 je často pouze 2 měsíce. Pokud správce v dokumentaci tvrdí, že data uchovává 14 měsíců (aby měl data pro roční srovnání), ale v nástroji má 2 měsíce, fakticky se dopouští nepřesnosti, ačkoliv tím nepoškozuje soukromí subjektů. Větším problémem by bylo, kdyby tvrdil 2 měsíce a měl nastaveno 14.

- **Doporučení:** Součástí implementace GDPR dokumentace musí být technický audit nastavení GA4 (Admin -> Data Settings -> Data Retention).

3. Právní základy a mechanismy souhlasu

Dokument 3 (Souhlas) a jeho vazba na Zásady zpracování odhaluje jemné právní nuance v oblasti marketingu.

3.1 Souhlas vs. Oprávněný zájem v marketingu

GDPR v bodě recitálu 47 explicitně uvádí, že "zpracování osobních údajů pro účely přímého marketingu lze považovat za zpracování prováděné z oprávněného zájmu". Český zákon č. 480/2004 Sb. (§ 7 odst. 3) to specifikuje tak, že pokud správce získá kontakt v souvislosti s prodejem, může jej využít pro nabídku vlastních obdobných výrobků/služeb (soft opt-in), dokud adresát nevyjádří nesouhlas.

- **Analýza šablony:** Šablona sází na jistotu a vyžaduje souhlas pro veškerý marketing. To je "nejčistší" cesta (hard opt-in), která eliminuje pochybnosti. Je však obchodně nevýhodná (nižší konverze, nutnost double opt-in).
- **Doporučení pro praxi:** Pokud má firma velkou bázi stávajících zákazníků, doporučuji přejít u této skupiny na *oprávněný zájem*. To vyžaduje úpravu Zásad (přidání oprávněného zájmu jako titulu pro marketing zákazníkům) a úpravu RoPA. Souhlas [4] by pak sloužil jen pro "nezákazníky" (odběratele newsletteru bez nákupu).

3.2 Profilování a čl. 22 GDPR

Dokumentace zmiňuje "Personalizaci obsahu a profilování" na základě souhlasu. To je správně. Článek 22 GDPR zakazuje pouze výhradně automatizované rozhodování s právními účinky bez lidského zásahu (např. automatické zamítnutí úvěru). Běžná marketingová personalizace (doporučení zboží) nemá "právní účinky" ani se subjektu "obdobně významně nedotýká" v intenzitě vyžadované čl. 22.23
Přesto, vyžádání souhlasu pro profilování (jak činí šablona) je bezpečnější cestou, zejména v kontextu pokynů EDPB, které zpřísňují pohled na cílenou reklamu (behaviorální reklamu). Šablona je zde nastavena konzervativně a bezpečně.

4. Řízení bezpečnostních incidentů (Incident Response)

Dokument 5 (Směrnice) je klíčový pro minimalizaci pokut. ÚOOÚ při stanovení výše pokuty zohledňuje, jak rychle a efektivně správce reagoval.

4.1 Kritéria rizika (Risk Assessment)

Šablona obsahuje jednoduchou matici pro posouzení rizika. To je v souladu s metodikou ENISA i ÚOOÚ. Klíčovým faktorem, který šablona správně zmiňuje, je **šifrování**. Pokud dojde ke ztrátě

notebooku, který je plně šifrován (BitLocker, FileVault), a klíč nebyl kompromitován, jedná se sice o bezpečnostní incident (narušení dostupnosti/důvěrnosti), ale zpravidla *nepředstavuje riziko* pro práva subjektů, a tedy se **nehlásí** ÚOOÚ ani subjektům.

- **Praktická poznámka:** Dokumentace by měla motivovat správce k zavedení šifrování koncových stanic. Bez technického opatření (šifrování) je směrnice jen papírovým drakem – každý ztracený telefon by se musel hlásit.

4.2 Vztah k NIS2

Zde se skrývá největší legislativní novinka let 2024/2025. Směrnice NIS2 a nový zákon o kybernetické bezpečnosti zavádí pro "regulované služby" povinnost hlásit incidenty do 24 hodin.

- **Proč je to problém:** Pokud firma spoléhá jen na tuto GDPR směrnici (72 hodin), může v případě kyberútoku (např. ransomware) promeškat lhůtu vůči NÚKIB. ÚOOÚ a NÚKIB sice spolupracují, ale povinnosti jsou samostatné.
- **Řešení v dokumentaci:** Do směrnice [4] doporučuji vložit bod: *"Před zahájením procesu hlášení ověřte, zda incident nenaplňuje znaky kybernetického bezpečnostního incidentu dle Zákona o kybernetické bezpečnosti. Pokud ano, postupujte prioritně dle havarijního plánu pro NIS2 (lhůta 24h)."*

---

5. Závěr a cesta k implementaci

Auditovaná dokumentace je **robustní, právně správná a aktuální**. Její autoři zjevně sledují vývoj legislativy a neuvízli v roce 2018. Šablony správně reagují na prodloužení retenčních lhůt u mezd i na uklidnění situace kolem přenosů dat do USA.

Pro finální nasazení doporučuji provést "lokalizaci" šablon – tedy nejen doplnit název firmy, ale i kriticky zhodnotit, zda firma využívá biometrii, zda má správně nastavené GA4 a zda nespadá pod NIS2. S těmito drobnými úpravami bude dokumentace představovat silný štít proti regulačním rizikům.

Citovaná díla

1. Statutory archiving period for payroll sheets extended by 15 years - Grant Thornton, použito prosince 28, 2025, https://www.grantthornton.cz/en/news/statutory-archiving-period-for-payroll-sheets-extended-by-15-years/
2. Archivace dat ve mzdové a personální oblasti | Ochrana osobních údajů a monitoring zaměstnanců, použito prosince 28, 2025, https://www.gdpr-vzory.cz/33/archivace-dat-ve-mzdove-a-personalni-oblasti-uniqueidmRRWSbk196FNf8-jVUh4Ens20EV5lG0TWUEplicJQRFK6fponjdgzQ/
3. Archivace mzdových listů a personálních dokladů, použito prosince 28, 2025,

https://www.archivace-dokumentu.cz/sluzby/mzdove-listy-archivace
4. 1-zasady-zpracovani-osobnich-udaju.pdf
5. Intuit - Data Privacy Framework, použito prosince 28, 2025, https://www.dataprivacyframework.gov/participant/7693
6. Google LLC - Data Privacy Framework, použito prosince 28, 2025, https://www.dataprivacyframework.gov/participant/5780
7. EUUS Data Privacy Framework Survives Legal Challenge What the Latombe Decision Means for Internation, použito prosince 28, 2025, https://www.twobirds.com/en/insights/2025/euus-data-privacy-framework-survives-legal-challenge-what-the-latombe-decision-means-for-internation
8. EU Court Upholds the Validity of the EU-U.S. Data Privacy Framework | The Data Advisor, použito prosince 28, 2025, https://www.wsgrdataadvisor.com/2025/09/eu-court-upholds-the-validity-of-the-eu-u-s-data-privacy-framework/
9. European General Court Upholds EU-U.S. Data Protection Framework | Enforcement Edge, použito prosince 28, 2025, https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2025/09/european-court-of-justice-upholds-eu-us-data-protection-framework
10. Průvodce novým zákonem o kybernetické bezpečnosti - Portál NÚKIB, použito prosince 28, 2025, https://portal.nukib.gov.cz/pruvodce-novym-zakonem-o-kyberneticke-bezpecnosti
11. Nový zákon o kybernetické bezpečnosti: Co musí firmy a jejich vedení udělat už nyní, použito prosince 28, 2025, https://arws.cz/novinky-v-arrows/novy-zakon-o-kyberneticke-bezpecnosti
12. Úkoly zaměstnavatelů při provádění důchodového pojištění - ePortál ČSSZ, použito prosince 28, 2025, https://eportal.cssz.cz/documents/20122/35802/ELDP_2012_Ukoly_zamestnavatelu_pri_provadeni_duchodoveho_pojisteni.pdf/801c1914-1891-10cb-5e81-c3a8180dc645?t=1737972027450
13. Archivace daňových dokladů: Co musíte uchovávat a jak ochránit firmu před sankcemi při kontrole? - ARROWS advokátní kancelář, použito prosince 28, 2025, https://arws.cz/novinky-v-arrows/archivace-danovych-dokladu
14. Prodloužení zákonné doby archivace mzdových listů | EY - Česká republika, použito prosince 28, 2025, https://www.ey.com/cs_cz/technical/tax/tax-alerts/2023/02/prodlouzeni-zakonne-doby-archivace-mzdovych-listu
15. Czech Republic, použito prosince 28, 2025, https://www.twobirds.com/en/trending-topics/global-cookie-review/czech-republic
16. Jak správně nastavit cookies lištu podle GDPR: Tipy z praxe analytika - Digitální architekti, použito prosince 28, 2025, https://digitalniarchitekti.cz/clanek/tipy-ke-cookies-z-praxe-analytika/
17. Data retention - Analytics Help, použito prosince 28, 2025, https://support.google.com/analytics/answer/7667196?hl=en

18. Understanding Data Retention Settings in GA4 - Cardinal Path, použito prosince 28, 2025, https://www.cardinalpath.com/blog/understanding-data-retention-settings-in-google-analytics
19. DEJTE SI POZOR NA DOUBLE OPT-IN U OBCHODNÍCH SDĚLENÍ (NEWSLETTERŮ), použito prosince 28, 2025, https://www.macek.legal/979/dejte-si-pozor-na-double-opt-in-u-obchodnich-sdeleni-newsletteru/
20. Povinnosti podnikatelů při zasílání obchodních sdělení zákazníkům - část I. - Právní prostor, použito prosince 28, 2025, https://www.pravniprostor.cz/clanky/obcanske-pravo/povinnosti-podnikatelu-pri-zasilani-obchodnich-sdeleni-zakaznikum-cast-i
21. Ohlášení porušení zabezpečení osobních údajů (data breach) - gov.cz, použito prosince 28, 2025, https://portal.gov.cz/sluzby-vs/ohlaseni-poruseni-zabezpeceni-osobnich-udaju-data-breach-S30277
22. Adequacy of the EU–U.S. Data Privacy Framework Survives Challenge - Workforce Bulletin, použito prosince 28, 2025, https://www.workforcebulletin.com/adequacy-of-the-eu-u-s-data-privacy-framework-survives-challenge
23. PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29, použito prosince 28, 2025, https://uoou.gov.cz/media/zahranici/dokumenty/schvalene-pokyny/k-profilovani.pdf