Zásady GDPR Metrostav Norge AS

1. Úvod

Metrostav Norge AS se zavazuje chránit právo na soukromí svých zaměstnanců a všech, s nimiž obchodně spolupracuje. Cílem tohoto dokumentu je stanovit zásady, podle kterých se bude nakládat s osobními údaji v souladu s platnými zákony o ochraně osobních údajů. To zahrnuje nařízení EU o ochraně osobních údajů 2016/679 (dále jen „GDPR“).

Za implementaci a monitorování postupu je odpovědný poradce pro ochranu osobních údajů ve společnosti Metrostav Norge AS.

2. Zásady ochrany dat

2.1. Obecně

Osobní údaje budeme zpracovávat v souladu s následujícími zásadami stanovenými v platné legislativě na ochranu soukromí a údajů.

2.2. Hlavní principy

Princip 1: Zákonnost, spravedlivost a transparentní informovanost

Spravedlivé nakládání: Zdržíme se zpracovávání osobních údajů způsobem, který je pro dotčené osoby nepřiměřeně škodlivý, neočekávaný nebo zavádějící.

Transparentní nakládání: Subjekty zpracovávání a uchovávání údajů budeme jasně, otevřeně a čestně informovat, za jakým účelem a jakým způsobem zpracováváme jejich osobní údaje.

Zákonnost: Zajistíme, aby veškeré zpracování osobních údajů mělo právní základ.

Princip 2: Omezení účelu

Osobní údaje budeme zpracovávat pouze pro konkrétní, explicitní a legitimní účely.

Konkrétní a explicitní: U každé činnosti zpracování určíme účel.

Legitimní: Účel musí být odůvodněný s ohledem na naše podnikání.

Nebudeme zpracovávat osobní údaje pro účely, které jsou neslučitelné s původním účelem, pro který byly osobní údaje shromážděny.

Anonymní údaje můžeme zpracovávat bez omezení, protože se již nejedná o osobní údaje.

Princip 3: Minimalizace dat

Budeme zpracovávat pouze osobní údaje, které jsou relevantní a nezbytné pro daný účel, a budeme:

• Identifikovat typy zpracovávaných osobních údajů, abychom mohli posoudit nezbytnost údajů.

• Instruujeme zaměstnance, aby se vyvarovali používání identifikátorů (pokud je to prakticky možné) a omezili množství osobních údajů v dokumentech a formulářích, ať už elektronických nebo tištěných.

Princip 4: Přesnost údajů

Přijmeme vhodná opatření, abychom zajistili, že osobní údaje jsou přesné, úplné a v případě potřeby aktuální. Abychom toho dosáhli:

• zavedeme vhodné postupy při shromažďování osobních údajů, aby byla zajištěna přesnost vkládaných údajů.

• zavedeme vhodné postupy pro pravidelné nebo ad-hoc kontroly systémů a dokumentů obsahujících osobní údaje, které vyžadují údržbu, aby byla zajištěna aktuálnost údajů.

• zavedeme vhodné postupy, které umožní subjektům zpracovávání údajů požadovat náhled a také jim umožní požadovat opravu, doplnění a aktualizaci jejich osobních údajů.

Princip 5: Omezení skladování

Osobní údaje nebudeme uchovávat déle, než je nezbytné pro účel, pro který byly shromážděny. Abychom toho dosáhli:

• stanovíme předpokládanou doby uchovávání (tedy kdy musí být osobní údaje vymazány), včetně důvodu doby uchovávání.

• implementujeme postupy automatického mazání v rozumném rozsahu.

• pokud bude rutiny mazání manuální, implementujeme harmonogram, systémy upozornění nebo jiné mechanismy, které zajistí dodržování rutin.

• podporujeme používání systémů/platforem pro archivaci a komunikaci s cílem omezit nestrukturovaná data.

• pokud jsou osobní údaje uchovávány pro latentní účely (např. k obhajobě potenciálních nároků), ale jinak nejsou potřebné pro každodenní provoz, budou přijata vhodná opatření k omezení přístupu k údajům a zabránění používání údajů v každodenním provozu (blokování nebo omezení přístupu). Je-li to možné, budou tato archivovaná data pseudonymizována (deidentifikována, např. nahrazením jména/identifikátoru ID).

• zvážíme anonymizaci jako alternativu k vymazání, pokud data mohou nadále sloužit účelu v anonymizované podobě. Anonymizace znamená, že data pravděpodobně nebudou znovu identifikovatelná běžnými prostředky.

• pokud systémová omezení vyžadují uchování záložních dat po uplynutí doby uchování dat, zajistíme, aby data v záloze podléhala přísné kontrole přístupu a nebyla provozně využívána.

Zásada 6: Integrita a důvěrnost

Zajistíme odpovídající zabezpečení osobních údajů, jak je dále popsáno níže.

3. Právní základ

3.1. Obecné

Identifikujeme platný právní základ pro každou činnost zpracování. Pokud nemůže být žádný právní základ identifikován jako platný, bude taková činnost ukončena.

Při zpracování osobních údajů, které nejsou zvláštními kategoriemi osobních údajů (citlivé osobní údaje), se můžeme podle článku 6 GDPR opřít o některý z následujících právních základů:

Právní základ	Popis	Požadavky	Příklady použití
Dohoda	Zpracování údajů je nezbytné pro splnění smlouvy se subjektem údajů nebo pro provedení kroků před uzavřením takové smlouvy.	Smlouva musí být uzavřena se subjektem údajů. Na tento právní základ se nelze spolehnout, jde-li o dohodu s obchodními partnery (právnickými osobami).	Nábor HR administrativa Mzdová agenda
Legitimní zájmy	Zpracování údajů je nezbytné pro dosažení oprávněného zájmu, pokud nad tímto zájmem nepřevažují práva a zájmy subjektů údajů.	Je identifikován oprávněný zájem nás nebo třetí strany (např. obchodního partnera); údaje jsou nezbytné k dosažení zájmu; a po zvážení zájmů oprávněný zájem převažuje nad právy a zájmy subjektu údajů.	Správa smluv s obchodními partnery Fúze a akvizice HR administrativa Mzdová agenda
Právní závazky	Zpracování údajů je nezbytné pro splnění zákonné povinnosti stanovené v právních předpisech členských států EU/EHP.	Právní povinnost musí být výslovně nebo implicitně stanovena v právu členského státu EU/EHP.	Účetnictví Bezpečnost
Životně důležité zájmy	Zpracování údajů je nezbytné pro ochranu životně důležitých zájmů subjektu údajů	Otázka života a smrti	Odezva v nouzové situaci
Veřejný zájem	Zpracování údajů je nezbytné pro plnění úkolů prováděných orgánem veřejné moci nebo soukromou organizací jednající ve veřejném zájmu.	Výkon úřední moci.	Veřejná informace

Právní základ	Popis	Požadavky	Příklady použití
Souhlas	Subjekt údajů souhlasil se zpracováním.	Souhlas musí být udělen v souladu s GDPR čl. 7.	Použití obrázků zaměstnanců na intranetu nebo internetu Uchovávání údajů o nevybraných uchazečích o zaměstnání po ukončení náborového procesu

3.2. Citlivé údaje

Pro zvláštní kategorie údajů (citlivé údaje) musíme mít navíc právní základ podle článku 9 GDPR. Citlivými údaji jsou údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení nebo členství v odborech a zpracování genetických údajů, biometrických údajů za účelem jednoznačné identifikace fyzické osoby, údajů o zdraví nebo údajů o sexuálním životě nebo sexuální orientaci fyzické osoby.

Při zpracování těchto citlivých osobních údajů identifikujeme některý z následujících právních základů:

Právní základ	Popis	Požadavky	Příklad použití
Zaměstnání	Zpracování údajů je nezbytné pro účely plnění povinností a výkonu konkrétních práv v oblasti pracovního práva a práva sociálního zabezpečení a sociální ochrany.	Musí být povoleno zákonem v každé členské zemi EU/EHP.	Vedení nemocenské. Upravení pracoviště ze zdravotních důvodů. Testy na alkohol nebo drogy na pracovišti, pokud jsou vyžadovány z bezpečnostních důvodů.
Životní zájmy	Zpracování údajů je nezbytné pro ochranu životně důležitých zájmů subjektu údajů v případě, že subjekt údajů není schopen dát souhlas.	Otázka života a smrti	Odezva v nouzové situaci
Veřejné údaje	Zpracování údajů se týká osobních údajů, které subjekt údajů zjevně zveřejňuje	Subjekt údajů musel údaje zjevně zveřejnit.	Public relations (např. zpracování příslušnosti k politické straně, kterou osoba zveřejnila).

Právní základ	Popis	Požadavky	Příklad použití
Právní závazky	Zpracování údajů je nezbytné pro určení, výkon nebo obhajobu právních nároků.	Nárok může být podložen zákonem, smlouvou nebo jinak.	Reagování na závazná předvolání orgánů veřejné moci.
Souhlas	Subjekt údajů se zpracováním výslovně souhlasil.	Souhlas musí být udělen v souladu s GDPR čl. 7.	Kontrola přístupu od dodavatele.

3.3. Trestní stíhání a odsouzení

Osobní údaje týkající se trestných činů a odsouzení můžeme zpracovávat pouze v případě, že mají právní základ, buď souhlas, zásadní zájem nebo právní nároky, jak je popsáno výše.

Údaje o odsouzeních za trestné činy jsou údaje týkající se osob odsouzených k trestu odnětí svobody, peněžitým trestům nebo jiným trestním sankcím soudy (nebo podobnými příslušnými institucemi), jakož i otázky a odpovědi týkající se toho, zda jednotlivec má či nemá záznam v trestním rejstříku. Údaje o trestných činech jsou údaje týkající se trestních obvinění nebo řízení.

3.4. Unikátní identifikátory

Rodná čísla a jiné jedinečné identifikátory smíme zpracovávat pouze v případě, že existuje odůvodněná potřeba určité identifikace a způsob je nezbytný k dosažení takové identifikace. Pro účely ověřování nebudeme zpracovávat čísla sociálního zabezpečení a jiné jedinečné identifikátory.

4. Transparentnost

4.1. Obecné

Budeme transparentní ohledně všech činností, při kterých dochází ke zpracování údajů a subjektům zpracovávání údajů poskytneme veškeré informace o ochraně osobních údajů.

4.2. Obsah informací o ochraně osobních údajů

Budeme informovat subjekty zpracovávání údajů o tom, proč a jak jsou jejich údaje zpracovávány, v souladu s článkem 13 a 14 GDPR. Informace musí být srozumitelné a jednoznačné. Informace o ochraně soukromí se pravidelně kontrolují, aby byla zajištěna jejich aktuálnost.

4.3. Sdělování informací o ochraně osobních údajů

Zajistíme, aby byly informace o ochraně osobních údajů snadno dostupné, například v rámci smluv a na našich webových stránkách. Na žádost subjektu údajů poskytneme také relevantní informace o ochraně osobních údajů.

4.4. Práva subjektu údajů

Budeme respektovat práva subjektů zpracování údajů, včetně práva na náhled, opravu, výmaz, omezení a práva vznést námitku.

4.5. Automatizované rozhodování

Můžeme používat automatizované rozhodování, včetně profilování, které má právní účinky na subjekty údajů nebo je obdobně ovlivňuje. Příkladem je automatizované posuzování žádostí o zaměstnání při náboru. Pro takové rozhodování splníme požadavky článku 22 GDPR.

4.6. Marketing

Můžeme provádět omezené marketingové aktivity. Přímý marketing můžeme zasílat e-mailem pouze následujícím příjemcům: těm, kteří souhlasili, nebo těm, kteří jsou stávajícími obchodními partnery. Příjemci budou mít možnost odhlásit se z budoucího e-mailového marketingu.

4.7. Ochrana soukromí již od návrhu a ochrana soukromí ve výchozím nastavení

Pokud vyvíjíme (vlastně nebo prostřednictvím poskytovatelů služeb) software, platformy nebo jiná řešení, zavedeme vhodná opatření určená k implementaci zásad ochrany dat jako integrovanou funkci. Nakonfigurujeme taková řešení tak, aby standardně omezovala množství osobních údajů, rozsah zpracování údajů a dobu uchovávání na minimum.

4.8. Společná kontrola

Společná kontrola existuje, když dva nebo více správců společně určují účely a prostředky zpracování, buď v rámci skupiny, nebo s ohledem na externí obchodní partnery.

Pokud my (jako správci) spolupracujeme s jedním nebo více dalšími správci (přidružená společnost nebo externí subjekt) v souvislosti se zpracováním osobních údajů, bude případ od případu posuzováno, zda jednají jako společní správci. Jako výchozí bod pro takové posouzení budeme považovat společnou kontrolu za pravděpodobnou, pokud strany sledují stejné celkové cíle a vzájemně přispívají ke zpracování údajů.

Pokud dojdeme k závěru, že existuje společná kontrola, bude uzavřena dohoda o společném správci. Taková dohoda určí příslušné odpovědnosti stran za dodržování platných zákonů a předpisů, včetně povinnosti poskytovat informace o ochraně soukromí subjektům údajů a role a odpovědnosti vůči subjektům údajů s ohledem na vyřizování žádostí o práva subjektů údajů.

5. Převod do zemí mimo EU/EHP

Všechny země v rámci regionu EU/EHP zavedly GDPR a zajistily tak správné nakládání s osobními údaji.

Aby bylo možné přenášet nebo zpracovávat osobní údaje mimo EU/EHP, musí být zajištěna odpovídající úroveň ochrany. To lze zajistit splněním standardních předpisů o ochraně osobních údajů přijatých Evropskou komisí (Standardní smluvní doložky).

6. Zpracovatelé dat s osobními údaji

Při zapojení zpracovatelů použijeme následující čtyřstupňový přístup:

Krok 1: Určení rolí

Nejprve určíme, zda daný subjekt jedná jako zpracovatel. Zpracovatel je společnost, která pro nás zpracovává osobní údaje, aniž by nezávisle určovala, proč ke zpracování dochází, jaké údaje mají být zpracovávány a jak dlouho mají být údaje uchovávány.

Krok 2: Prověřování

Před zapojením zpracovatele ověříme, že zpracovatel poskytuje dostatečné záruky pro splnění požadavků platných zákonů o ochraně osobních údajů. Můžeme tak učinit vyžádáním příslušné dokumentace a informací o ochraně osobních údajů v procesu zadávání veřejných zakázek nebo jinými vhodnými prostředky.

Krok 3: Uzavření smlouvy o zpracování údajů

S každým zpracovatelem uzavřeme smlouvu o zpracování údajů / smlouvu o správě informací. Taková smlouva může tvořit dodatek k jiné smlouvě (jako je smlouva o poskytování služeb).

Krok 4: Audit

Ověříme dodržování smlouvy o zpracování údajů.

Můžeme požádat zpracovatele, aby pravidelně připravoval zprávy o zabezpečení dat. Zkontrolujeme zprávu a posoudíme přiměřenost opatření pro zabezpečení údajů a soukromí. Pokud zpráva odhalí varovné signály, požádáme o další informace. Máme-li důvod se domnívat, že standardy zabezpečení dat nebo ochrany soukromí zpracovatele jsou nedostatečné, provedeme důkladnější audit. Pokud nejsme spokojeni s úrovní zabezpečení dat nebo standardů ochrany soukromí, ukončíme smlouvu.

7. Sdílení dat s nezávislými správci

Kdykoli jako správce sdílíme osobní údaje s jiným samostatným správcem, zvážíme to formalizovat dohodou o ochraně osobních údajů před nezákonným zpracováním.

Kdykoli jako správce obdržíme osobní údaje od jiného samostatného správce, zvážíme uložení smluvní povinnosti takovému správci oznámit subjektům údajů skutečnost, že jsme příjemcem osobních údajů, abychom takového správce podpořili v souladu s GDPR. článek 13.

8. Záznamy o činnostech zpracování

Zavedeme záznamy o činnostech zpracování. Účelem těchto záznamů je zajistit soulad s článkem 30 GDPR a usnadnit soulad s dalšími požadavky GDPR. Při vytváření záznamů o činnostech zpracování se použije šablona norského dozorčího úřadu Arbeidstilsynet.

Je odpovědností každého vlastníka zpracování údajů, aby takové záznamy doplnil a udržoval. Vlastník zpracování dat je role, která má funkční odpovědnost.

9. Zabezpečení dat

Zavedeme a budeme udržovat vhodná technická a organizační opatření, abychom zajistili odpovídající úroveň zabezpečení údajů, abychom zabránili náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zpřístupnění přenášených, uchovávaných nebo jinak zpracovávaných osobních údajů nebo přístupu k nim.

U osobních údajů zajistíme, aby opatření k zabezpečení údajů náležitě zohledňovala následující aspekty:

Bezpečnostní kritéria	Definice	Popis / Příklady
Důvěrnost	Ochrana před neoprávněným přístupem nebo zveřejněním dat.	1. Zaměstnanci a obchodní partneři budou podléhat přiměřené povinnosti mlčenlivosti. 2. Databáze budou zašifrovány a budou podléhat odpovídající kontrole přístupu. 3. Dohody s prodejci IT budou zahrnovat závazky v oblasti zabezpečení dat. 4. Fyzická zařízení budou přiměřeně chráněna proti neoprávněnému přístupu.
Integrita	Ochrana proti neoprávněným úpravám nebo vymazání dat.	1. Databáze budou zašifrovány a budou podléhat odpovídající kontrole přístupu. 2. Klíčové dokumenty budou mít kontrolu verzí (historii revizí).
Přístupnost	Přístup k údajům v případě potřeby.	1. Dohody s klíčovými poskytovateli IT služeb budou mít odpovídající podmínky. 2. Materiálová data budou vzdáleně přístupná (VPN nebo podobně).
Odolnost	Kontinuita podnikání je zajištěna	1. Dohody s klíčovými poskytovateli IT služeb budou mít odpovídající obchodní podmínky. 2. Data budou zálohována.

10. Řešení úniku dat

Potenciálně můžeme zaznamenat porušení zabezpečení osobních údajů – porušení zabezpečení vedoucí k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zveřejnění osobních údajů nebo přístupu k nim. Pokud k tomu dojde, do 72 hodin posoudíme, zda musíme informovat subjekty údajů a/nebo příslušný úřad pro ochranu údajů.

Zaměstnanci, kteří podezřívají nebo zjistí nežádoucí incidenty související se zpracováním osobních údajů, neprodleně oznámí incident svému přímému nadřízenému, personalistovi nebo poradci pro ochranu osobních údajů. Za informování příslušného úřadu pro ochranu osobních údajů je odpovědný poradce pro ochranu osobních údajů.

11. Posouzení rizika ochrany soukromí

Pravidelně budeme provádět obecné hodnocení rizika ochrany soukromí našeho podnikání. Účelem takového hodnocení je identifikovat potenciální rizika pro soukromí a identifikovat opatření vhodná k minimalizaci těchto rizik. V kontextu soukromí jsou rizika (nežádoucí následky události) zejména: Fyzické poškození; Diskriminace; Krádež identity; Podvod; Finanční ztráta; Poškození pověsti; ekonomické nebo sociální znevýhodnění; neoprávněné zveřejnění nebo přístup ke zvláštním kategoriím údajů; Neoprávněné zveřejnění nebo přístup k údajům týkajícím se osobních aspektů, jako je ekonomická situace nebo hodnocení pracovního výkonu.

Posouzení rizik by mělo brát v úvahu alespoň: (i) úroveň přijatelného rizika, (ii) potenciální nežádoucí události, (iii) pravděpodobnost výskytu těchto událostí, (iv) důsledky pro soukromí, pokud k události dojde, a (iv), pokud je riziko nepřijatelné, opatření k řešení rizika.

12. **Posouzení vlivu na ochranu údajů**

Pokud operace zpracování, jako je použití nové technologie, pravděpodobně povede k vysokému riziku ochrany soukromí s ohledem na její povahu, rozsah, kontext a účel, provedeme posouzení vlivu na ochranu údajů (DPIA).

DPIA musí obsahovat alespoň i) systematický popis zamýšlené operace zpracování, ii) posouzení její nezbytnosti a přiměřenosti, iii) posouzení rizik pro soukromí a iv) opatření k řešení rizik.

13. Identifikace hlavního dozorčího orgánu

Je-li vyžadována komunikace s dozorčí úřadem v souvislosti s přeshraničním zpracováním údajů, které zahrnuje více než jednu zemi EHP, musí být určen hlavní dozorčí úřad.

Orgán dozoru je orgán země, ve které se nachází naše hlavní provozovna. Hlavní provozovna se nachází v místě naší ústřední správy, pokud nejsou rozhodnutí týkající se účelů a prostředků zpracování přijímána v jiné provozovně, která má pravomoc taková rozhodnutí provádět.

14. Školení

Našim zaměstnancům poskytneme školení o ochraně dat a soukromí.

Pracovníci s trvalým nebo pravidelným přístupem k osobním údajům, kteří se podílejí na shromažďování osobních údajů nebo na vývoji nástrojů používaných ke zpracování osobních údajů, absolvují povinná školení o ochraně soukromí a údajů. Příslušní pracovníci by měli být definováni podle toho, jak jsou vystaveni zpracování osobních údajů v rámci své pozice a každodenních úkolů. Příslušní pracovníci jsou:

• HR oddělení, které spravuje personální data.

• Bezpečnostní funkce, konkrétněji personál v rámci zdraví a pracovního prostředí, personál řešící bezpečnostní incidenty zahrnující identifikované jednotlivce a personální týmy reakce na mimořádné události

• Firemní audit

• IT funkce, konkrétněji pracovníci věnující se bezpečnosti informací, podpoře aplikací a dalším meziskupinovým IT službám

• Linioví manažeři