

SMLOUVA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE ČL. 28 ODS. 3 GDPR

Objednatel (správce):

Jméno a příjmení kooperačního partnera

Číslo kooperačního partnera

Obchodní název firmy

Ulice, číslo popisné

PSČ, město/obec

Zhotovitel (zpracovatel):

ThomasLloyd Global Asset Management GmbH
Hanauer Landstraße 291b
60314 Frankfurt am Main
Německo

1. Předmět a doba platnosti dohody

Pověření zpracováním zahrnuje:

Pravidelně se opakující provádění mailingových akcí podle příslušné jednotlivé objednávky; zaslání pošty klientům a zájemcům správce (adresy přenechá správce), kontrola adresových souborů ohledně způsobilosti k zaslání, kontrola duplicity prováděná z pověření správce formou porovnání; personalizace poštovních zásilek s ohledem na správce; předání korekturního otisku správci ke schválení; bezplatné rozeslání pošty.

Zhotovitel na základě této smlouvy zpracovává osobní údaje pro objednatele ve smyslu čl. 4 č. 2 a čl. 28 GDPR.

Zpracování údajů realizované v rámci této smlouvy o zpracování osobních údajů se v zásadě provádí ve Spolkové republice Německo, v některém z členských států Evropské unie nebo v jiném smluvním státě Dohody o evropském hospodářském prostoru (EHS) nebo ve Švýcarsku. Zhotoviteli je rovněž povoleno zpracovávat osobní údaje objednatele při dodržení ustanovení této dohody také v zemích mimo EHS, pokud zhotovitel objednatel o této skutečnosti a o místě zpracování údajů včas předem informoval a pokud jsou splněny zvláštní předpoklady stanovené v čl. 44 až 48 GDPR nebo je dána výjimka podle čl. 49 GDPR. Švýcarsko poskytuje dle rozhodnutí Evropské komise o odpovídající ochraně adekvátní úroveň ochrany osobních údajů ve smyslu čl. 44 a násl. GDPR.

2. Doba platnosti pověření

Smlouva vstupuje v účinnost jejím podpisem oběma smluvními stranami. Závazek z této smlouvy zaniká výpovědí jedné ze smluvních stran. Vypovězení smlouvy musí být provedeno v písemné formě při dodržení výpovědní doby 4 týdnů.

Objednatel může smlouvu kdykoli vypovědět bez dodržení výpovědní doby, jestliže zhotovitel závažným způsobem poruší předpisy o ochraně osobních údajů nebo ustanovení této smlouvy nebo jestliže nemůže či nechce provést pokyn objednatele nebo v rozporu s touto smlouvou odmítá práva objednatele na kontrolu. Závažným porušením se přitom rozumí zejména nedodržení povinností vyplývajících z této smlouvy a z čl. 28 GDPR.

3. Povaha a účel zpracování, druh osobních údajů a kategorie subjektů údajů:

Povaha zpracování (podle definice obsažené v čl. 4 č. 2 GDPR):

- převzetí a uložení záznamů kontaktních údajů (jméno, adresa, e-mailová adresa) klientů a zájemců správce, kteří mají být osloveni
- kontrola duplicity formou porovnání
- rozeslání propagačních zásilek vztahujících se k příslušné „e-mailingové akci ThomasLloyd“ nebo „mailingové akci ThomasLloyd“

Druh osobních údajů (podle definice obsažené v čl. 4 č. 1, 13, 14 a 15 GDPR):

- záznamy kontaktních údajů (jméno, adresa, e-mailová adresa) klientů a zájemců správce, kteří mají být osloveni

Kategorie subjektů údajů (podle definice obsažené v čl. 4 č. 1 GDPR):

- klienti nebo zájemci správce

4. Práva a povinnosti objednatele a jeho oprávnění k vydávání pokynů

Posouzení přípustnosti zpracování podle čl. 6 odst. 1 GDPR a ochrana práv subjektů údajů podle čl. 12 až 22 GDPR spadá do výhradní odpovědnosti objednatele. Zhotovitel je zároveň povinen předat objednateli veškeré dotazy týkající se této záležitosti, jestliže je z nich patrné, že jsou určeny výhradně objednateli.

Změny předmětu zpracování a změny postupů musejí být společně ujednány mezi objednatel a zhotovitelem a musejí být zachyceny písemně nebo v doloženém elektronickém formátu.

Objednatel zpravidla uděluje veškerá pověření, dílčí pověření a pokyny písemně nebo v doloženém elektronickém formátu. Ústní pokyny je nutno neprodleně potvrdit písemně nebo v doloženém elektronickém formátu.

Objednatel má právo se přesvědčit o dodržování technických a organizačních opatření, která zhotovitel přijal a která jsou uvedena v Příloze 1, jakož i o dodržování povinností stanovených touto smlouvou. Objednatel se před zahájením zpracování se o těchto skutečnostech přesvědčí tak, jak je stanoveno v bodě 6, a poté je oprávněn dodržování opatření a povinností přiměřeným způsobem ověřovat pravidelně. Objednatel bude zhotovitele neprodleně informovat v případě, že při kontrole výsledků zpracování zjistí pochybení či nepřesnosti.

Smluvní partneri jsou povinni zachovávat mlčenlivost o všech obchodních tajemstvích příslušného druhého smluvního partnera a všech jeho opatřeních na zabezpečení údajů, o kterých se v rámci smluvního vztahu dozví. Tato povinnost trvá i po ukončení této smlouvy.

5. Osoby oprávněné vydávat pokyny na straně objednatele, příjemce pokynů na straně zhotovitele

Osobami oprávněnými vydávat pokyny na straně objednatele jsou:

Jméno, příjmení, organizační jednotka, telefon

Jméno, příjmení, organizační jednotka, telefon

Příjemcem pokynů na straně zhotovitele je příslušná kontaktní osoba, která byla objednateli určena.

V případě, že dojde ke změně kontaktní osoby nebo že nebude kontaktní osoba delší dobu k zastížení, je nutno smluvnímu partnerovi sdělit nástupce resp. zástupce, a to zásadně písemně nebo elektronicky. Pokyny je nutno uchovávat po celou dobu jejich platnosti a poté ještě tři celé kalendářní roky.

6. Povinnosti zhotovitele

Zhotovitel zpracovává osobní údaje výhradně v rámci uzavřených dohod a podle pokynů objednatele, pokud mu toto zpracování již neukládá za účelem jiného zpracování unijní právo nebo právo státu, které se na zpracovatele vztahuje (jedná se např. o šetření orgánů trestního stíhání nebo orgánů státní ochrany); v takovém případě zpracovatel správce o tomto právním požadavku informuje před zpracováním, leda že by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu (čl. 28 odst. 3 věta 2 písm. a) GDPR).

Zhotovitel nepoužívá osobní údaje přenechané ke zpracování pro žádné jiné účely, zejména ne pro účely vlastní. Kopie nebo duplikáty osobních údajů se bez vědomí objednatele nepořizují.

Zhotovitel v rámci zpracování osobních údajů, prováděného v souladu s pověřením, zajistí realizaci všech sjednaných opatření podle smlouvy. Zhotovitel zajistí, aby byly údaje, které jsou zpracovávány pro objednatele, striktně odděleny od ostatních datových souborů.

Nosiče dat, které pocházejí od objednatele resp. které jsou používány pro objednatele, budou zvlášť označeny. Vstup a výstup i běžné používání se zadokumentuje.

Zhotovitel je povinen po celou dobu poskytování služby pro objednatele provádět na svém úseku tyto kontroly:

- kontroly dodržování a realizace technických a organizačních opatření stanovených v přílohách;
- výsledek kontrol je nutno zadokumentovat.

Zhotovitel je při plnění práv subjektů údajů podle čl. 12 až 22 GDPR prostřednictvím objednatele, při sestavování záznamů o činnostech zpracování i při nezbytném posuzování vlivu na ochranu osobních údajů prostřednictvím objednatele povinen poskytnout součinnost v nezbytném rozsahu a objednatel pokud možno přiměřeně podporovat (čl. 28 odst. 3 věta 2 písm. e) a f) GDPR).

Zhotovitel vždy neprodleně upozorní objednatele na to, že pokyn udělený objednatelem dle jeho názoru porušuje zákonné předpisy (čl. 28 odst. 3 věta 3 GDPR). Zhotovitel má právo pozastavit provádění příslušného pokynu do té doby, než jej objednatel potvrdí nebo změní.

Zhotovitel je povinen osobní údaje získané ze smluvního vztahu opravit nebo vymazat či omezit jejich zpracování, pokud to bude objednatel prostřednictvím pokynu požadovat a pokud to nebude v rozporu s oprávněnými zájmy zhotovitele.

Zhotovitel smí poskytovat informace o osobních údajích získaných ze smluvního vztahu třetím stranám nebo subjektům údajů pouze na základě předchozího pokynu nebo souhlasu objednatele.

Zhotovitel vyjadřuje svůj souhlas s tím, aby měl objednatel právo v přiměřeném a nezbytném rozsahu kontrolovat - zásadně po sjednání termínu, a sice buď sám, nebo prostřednictvím třetích osob, které pověří - dodržování předpisů o ochraně osobních údajů a zabezpečení údajů a dodržování smluvních ujednání. Tuto kontrolu může objednatel provádět zejména prostřednictvím obstarání informací, nahlédnutí do uložených údajů a programů pro zpracování údajů a prostřednictvím auditů a inspekcí na místě (čl. 28 odst. 3 věta 2 písm. h) GDPR).

Zhotovitel zaručuje, že bude v případě potřeby poskytovat při těchto kontrolách součinnost a podporu.

Zpracování údajů v soukromých bytech (práce zaměstnanců zhotovitele z domova nebo po telefonu) není dovoleno.

Zhotovitel potvrzuje, že jsou mu známa příslušná ustanovení nařízení GDPR o ochraně osobních údajů, která se vztahují na pověření zpracováním osobních údajů.

Zhotovitel se zavazuje, že bude při zpracování osobních údajů objednatele, prováděném v souladu s pověřením, zachovávat důvěrný charakter údajů. Tato povinnost trvá i po ukončení smlouvy.

Zhotovitel zaručuje, že před zahájením činnosti seznámí pracovníky, kteří se budou podílet na provádění prací, s příslušnými ustanoveními o ochraně osobních údajů a že je na dobu jejich činnosti i na dobu po ukončení zaměstnaneckého poměru přiměřeným způsobem zaváže k mlčenlivosti (čl. 28 odst. 3 věta 2 písm. b) a čl. 29 GDPR). Zhotovitel ve své společnosti dohlíží na dodržování právních předpisů o ochraně osobních údajů.

Pověřencem/pověřenci pro ochranu osobních údajů je/jsou na straně zhotovitele jmenován/jmenováni

- **pan Andreas Obrist**, ThomasLloyd Global Asset Management (Schweiz) AG; Uraniastrasse 35, 8001 Zürich;
e-mail: gdpr@thomas-lloyd.com

Změnu pověření pro ochranu osobních údajů je objednateli nutno neprodleně oznámit.

7. Oznamovací povinnosti zhotovitele v případě narušení zpracování a porušení ochrany osobních údajů

Zhotovitel objednateli neprodleně oznámí případy narušení zpracování či porušení právních ustanovení o ochraně osobních údajů nebo ustanovení sjednaných v rámci pověření dle této smlouvy, způsobené zhotovitelem nebo osobami, které zhotovitel zaměstnává. Rovněž zhotovitel neprodleně oznámí objednateli podezření na porušování ochrany osobních údajů nebo podezření na nepřesnosti při zpracování osobních údajů. To platí především také s ohledem na případné ohlašovací a oznamovací povinnosti objednatele podle čl. 33 a 34 GDPR. Zhotovitel zaručuje, že bude objednatel v případě potřeby přiměřeně podporovat (čl. 28 odst. 3 věta 2 písm. f) GDPR) při plnění jeho povinností podle čl. 33 a 34 GDPR. Ohlášení podle čl. 33 nebo oznámení dle čl. 34 GDPR smí zhotovitel za objednatele činit pouze na základě předchozího pokynu podle bodu 4 této smlouvy.

8. Smluvní vztahy se subdodavateli (čl. 28 odst. 3 věta 2 písm. d) GDPR)

Objednatel tímto uděluje zhotoviteli všeobecné povolení k tomu, aby s ohledem na zpracování osobních údajů dle této smlouvy zapojil další zpracovatele (dále jen „subdodavatelé“), zejména pak společnosti náležející do skupiny zhotovitele, jako je např. ThomasLloyd Global Asset Management (Schweiz) AG. V případě, že dojde k zapojení společností ve skupině, které sídlí v třetí zemi, bude zhotovitel objednatel zvlášť informovat o přijatých opatřeních na zabezpečení přiměřené úrovně ochrany osobních údajů podle článku 44 a násl. GDPR.

Zhotovitel svá smluvní ujednání se subdodavateli zakotví do písemné smlouvy tak, aby smluvní povinnosti a případné doplňující pokyny, které se na zhotovitele vztahují podle této dohody, platily i vůči subdodavatelům. Smluvní strany sjednávají, že se tento požadavek považuje za splněný tehdy, jestliže smluvní ujednání se subdodavatelem vykazují úroveň ochrany, jež odpovídá této dohodě, resp. jestliže jsou subdodavateli uloženy povinnosti, které předepisuje čl. 28 odst. 3 GDPR.

Za subdodavatelské vztahy ve smyslu předchozích ustanovení se nepovažují služby, které zhotovitel využije u třetích stran jako vedlejší službu za účelem podpory při provádění zpracování, jímž byl pověřen. Patří sem například telekomunikační služby, úklidové služby nebo dle okolností také kontrolní a údržbové služby, třebaže při nich nelze vyloučit přístup k osobním údajům objednatele. Zhotovitel i v případě takovýchto externě zadávaných vedlejších služeb zavede přiměřená pravidla na ochranu důvěrného charakteru údajů objednatele.

Při dodržení požadavků stanovených v bodě 1 této dohody platí ustanovení obsažená v tomto bodě 8 i tehdy, jestliže dojde k zapojení subdodavatele v třetí zemi. Objednatel souhlasí s tím, že poskytne součinnost při plnění zvláštních předpokladů stanovených v článku 44 a násl. GDPR.

9. Technická a organizační opatření podle čl. 32 GDPR (čl. 28 odst. 3 věta 2 písm. c) GDPR)

Pro konkrétní zpracování je zaručena přiměřená úroveň ochrany odpovídající danému riziku pro práva a svobody fyzických osob, jichž se zpracování dotýká. Cíle ochrany stanovené v čl. 32 odst. 1 GDPR – jako je důvěrnost, integrita a dostupnost systému a služeb a jejich odolnost s ohledem na druh, rozsah, okolnosti a účel

zpracování – jsou při tom zohledněny tak, aby bylo toto riziko pomocí vhodných technických a organizačních nápravných opatření trvale sníženo.

Technická a organizační opatření pro ochranu a zabezpečení osobních údajů, která jsou přijata zhotovitelem a jsou popsána v Příloze 1, představují podrobný výběr technických a organizačních opatření odpovídajících zjištěnému riziku s přihlédnutím k cílům ochrany a ke stavu techniky a se zvláštním přihlédnutím k IT systémům a k procesům zpracování používaných na straně zhotovitele.

Zhotovitel bude v rámci daného podnětu, nejméně však v ročním intervalu, provádět testování, posuzování a hodnocení účinnosti technických a organizačních opatření dle Přílohy 1 pro zajištění bezpečnosti zpracování (čl. 32 odst. 1 písm. d) GDPR). Výsledek včetně kompletní zprávy z auditu oznámí objednateli.

V případě, že nastane potřeba zdokonalit či upravit technická a organizační opatření, bude zhotovitel o této skutečnosti neprodleně informovat objednatele. Zhotovitel rovněž bude objednatel podporovat při tvorbě dokumentace o dodržování nezbytných technických a organizačních opatření podle čl. 32 GDPR. Bude-li v rámci kontroly provedené ze strany objednatele před zahájením zpracování nebo během zpracování zjištěno, že nastala potřeba zdokonalení či úpravy technických a organizačních opatření nebo že je třeba opatření zdokonalit či upravit z jiných důvodů, splní tuto potřebu zhotovitel a její splnění zadokumentuje. Dokumentaci pak předá objednateli. Zadokumentovaná opatření se stanou součástí a základem této smlouvy.

Zhotovitel a objednatel přijmou na základě vzájemné dohody rozhodnutí, která se vztahují k organizaci zpracování osobních údajů a k uplatňovaným postupům, a která jsou významná pro bezpečnost zpracování.

Pokud nebudou opatření přijatá zhotovitelem vyhovovat požadavkům objednatele, bude objednatel o této skutečnosti zhotovitele neprodleně informovat.

Opatření přijatá zhotovitelem mohou být v průběhu smluvního vztahu přizpůsobována dalšímu technickému a organizačnímu vývoji, jejich úroveň však nesmí být nižší, než jsou sjednané standardy. Zásadní změny musí zhotovitel v doložené formě (písemně, elektronicky) dohodnout s objednatel. Tyto dohody je nutno uchovávat po celou dobu trvání této smlouvy.

10. Povinnosti zhotovitele po ukončení pověření ke zpracování, čl. 28 odst. 3 věta 2 písm. g) GDPR

Zhotovitel je po ukončení této dohody povinen vydat objednateli veškeré údaje, podklady a výsledky zpracování a použití, které v souvislosti se zpracováním osobních údajů dle této smlouvy získal, nebo je na žádost objednatele vymazat resp. zničit/nechat zničit.

Výmaz resp. zničení je nutno objednateli potvrdit písemně nebo v doloženém elektronickém formátu s uvedením data výmazu či zničení osobních údajů.

11. Odpovědnost

Je odkazováno na čl. 82 odst. 1 GDPR. V ostatních ohledech se sjednává následující:

Pokud je za škodu podle čl. 82 odst. 2 GDPR odpovědný jak objednatel, tak zhotovitel, odpovídají smluvní partneri za tuto škodu v rámci vnitřního vztahu podle svých podílů na odpovědnosti. Uplatní-li nějaká osoba v takovém případě vůči jednomu ze smluvních partnerů nárok na celou náhradu škody nebo nárok na náhradu škody přesahující podíl dotčeného smluvního partnera na odpovědnosti, může tento smluvní partner od příslušného druhého smluvního partnera požadovat zproštění odpovědnosti nebo odškodnění, pokud náhrada škody přesahuje jeho podíl na odpovědnosti.

12. Ostatní ustanovení

Oba smluvní partneri budou dohody o technických a organizačních opatřeních a kontrolní a zkušební dokumentaci uchovávat po dobu jejich platnosti a následně ještě tři celé kalendářní roky. Pro vedlejší ujednání se zásadně požaduje písemná forma nebo doložený elektronický formát.

Pokud by u zhotovitele došlo v důsledku opatření třetích stran (např. obstavení nebo zabavení majetku), insolvenčního řízení či v důsledku jiných událostí k ohrožení vlastnictví nebo ohrožení osobních údajů objednatele určených ke zpracování, je zhotovitel povinen objednatele o této skutečnosti neprodleně informovat.

Námitka zadržovacího práva ve smyslu § 273 BGB (německého občanského zákoníku) je, co se týče údajů zpracovávaných pro objednatele a příslušných nosičů dat, vyloučena.

Pokud by byly jednotlivé části této dohody neúčinné, zůstává tím účinnost ostatních částí dohody nedotčena.

Podpisy:

Objednatel

Zhotovitel

Příloha 1: Technická a organizační opatření pro ochranu osobních údajů a pro zabezpečení údajů na straně zhotovitele

PŘÍLOHA 1

KE SMLouvĚ O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PODLE ČL. 28 Odst. 3 GDPR

Popis technických a organizačních opatření pro ochranu osobních údajů a zabezpečení údajů ve společnosti ThomasLloyd

Podle čl. 28 odst. 3 GDPR je nutno technická a organizační opatření pro ochranu osobních údajů, která mají být přijata v souladu s čl. 32 GDPR, stanovit písemně.

Realizaci a dodržování níže uvedených technických a organizačních opatření ověřuje v rámci pravidelných kontrol pověřenec společnosti ThomasLloyd pro ochranu osobních údajů.

1. Kontrola vstupu

Opatření, která nepovolaným osobám zabraňují v přístupu k materiálům, jejichž pomocí jsou osobní údaje zpracovávány nebo používány:

- Vstupní dveře do kanceláře jsou neustále zamčené (během pracovní doby i mimo ni).
- Je prováděna elektronická kontrola vstupu pomocí čipu a o této kontrole je pořizován záznam do protokolu.
- Přidělení čipu a klíče se dokumentuje.
- Vstupní prostor se nachází ve viditelném dosahu pracovníků sekretariátu a recepce.
- Externí osoby se směřjí a mohou po kanceláři pohybovat pouze za neustálého doprovodu.
- Návštěvníci jsou zaznamenáváni do knihy návštěv.
- Mimo pracovní dobu kanceláře je zapnuto poplašné zařízení; elektronická kontrola vstupu pomocí čipu je zablokována.
- Vstup do serveroven a místností určených pro provoz sítě je umožněn pouze vedoucím pracovníkům IT a jejich zástupcům.

2. Kontrola přístupu

Opatření, která nepovolaným osobám zabraňují v používání systémů na zpracování dat:

- Veškeré systémy na zpracování dat lze používat pouze po zadání uživatelského jména a hesla.
- Uživatelské jméno a heslo se přiděluje individuálně.
- Hesla jsou důvěrná a musejí vykazovat minimální délku.
- Hesla musejí být pravidelně měněna.
- Stejně heslo nelze použít vícekrát.
- Po 20 minutách nečinnosti dochází k zablokování pracovní stanice; zablokování může zrušit pouze přihlášený uživatel nebo administrátor.
- Administraci serverových systémů lze provádět pouze na řídicím panelu nebo přes šifrované spojení.
- Serverové systémy jsou chráněny různými hesly.
- Přístup k datům a procesům serverových systémů je možný pouze v rámci interní sítě; komunikace s externími klienty neprobíhá. Zabezpečení před externím přístupem je zajištěno prostřednictvím dvouúrovňové koncepce firewallu, včetně systému detekce průniku (Intrusion Detection System - IDS) se softwarem od různých výrobců.
- Je prováděno dvojí antivirové testování pomocí softwaru od různých výrobců, přičemž aktualizace signatur probíhá přinejmenším denně.
- Je prováděn kompletní antivirový test založený na konkrétních pravidlech.

3. Kontrola přístupu a zásahu

Opatření na zajištění toho, aby měly osoby, jež jsou oprávněny k užívání systému na zpracování dat, přístup výhradně k těm údajům, které spadají pod jejich oprávnění k přístupu, a aby při zpracování a užívání osobních údajů a po jejich uložení nemohlo dojít k neoprávněnému čtení, kopírování, provedení změn nebo k odstranění těchto údajů.

- Zřízení osobních účtů pracovníků.
- Udělování oprávnění k přístupu pouze těm pracovníkům, kteří se na užívání bezprostředně podílejí, přičemž přístup je umožněn výhradně jen k údajům, které jsou nezbytné pro splnění příslušných úkolů (systém přístupových práv založený na konkrétních úkolech).
- Práva centrálně uděluje administrátor systému, a to samostatně podle vyvolání souboru, vyhotovení, psaní, provádění úprav, vymazání, čtení a řízení přístupu.
- Práva k přístupu se udělují podle skupinových směrnic, ve výjimečných případech individuálně.

- Práva lze udělovat krátkodobě a lze je znovu odnímat.
- Práva jsou s ohledem na pracovní stanice a servery ověřována při každé autentizaci.
- Nařízení ohledně schvalování smí vydávat pouze vedení společnosti resp. pracovníci odpovědní za oblast dat.
- Přístupová oprávnění jsou zaznamenávána do protokolu.
- Jednoznačná identifikace počítačů serverem prostřednictvím kontroly IP adresy.
- Ochrana pracovních stanic před neoprávněnými změnami hardwaru nebo softwaru.
- Neustále aktualizovaná ochrana pracovních stanic a serverů před napadením viry a malwarem.
- Zabezpečení intranetu prostřednictvím průběžně udržovaného a monitorovaného víceúrovňového firewallu a systému detekce průniku.
- Omezený přístup k internetu (založený na konkrétních pravidlech).

4. Kontrola předávání

Opatření na zajištění toho, aby při elektronickém přenosu osobních údajů nebo během jejich transportu či ukládání na nosiče dat nemohlo dojít k neoprávněnému čtení, kopírování, provedení změn nebo k odstranění těchto údajů, a aby bylo možno prověřit a zjistit, na jaká místa mají být osobní údaje prostřednictvím zařízení pro přenos dat přeneseny:

- Elektronický přenos údajů probíhá podle konkrétních dohod s oprávněnými příjemci.
- Osobní údaje jsou přenášeny prostřednictvím internetového serveru zabezpečeného certifikátem SSL („bezpečnostní schránka na dokumenty“) (https, zabezpečeno vysokostupňovým šifrováním, RSA 2048 bitů, signováno prostřednictvím Verisign).
- Přístup k bezpečnostní schránce na dokumenty je možný pouze přes osobní účty.
- Na pracovních stanicích nedochází k ukládání údajů.
- Údaje se ukládají na zabezpečené nosiče dat (servery) v počítačové místnosti, a to výhradně přes intranet.
- Na přenosné nosiče dat (diskety, CD, USB flash disky atd.) se osobní údaje neukládají.
- Ostatní údaje (např. prezentace) se na přenosné nosiče dat (diskety, CD, USB flash disky atd.) ukládají, avšak jejich ukládání provádějí pouze pověřeni pracovníci.
- Přepisovatelné přenosné nosiče dat (USB flash disky) se po použití odevzdávají grafickému oddělení, v němž se provádí vymazání údajů, které se na těchto nosičích nacházejí.
- Zničení přenosných nosičů dat provádí po jejich použití externí certifikovaný poskytovatel služeb (documentus GmbH Berlin & Co. Betriebs KG).
- V rámci firemní sítě je zakázáno používat vlastní notebooky, USB flash disky či hard disky.
- Příslušná rozhraní na pracovních stanicích (např. USB ovladač, disketové jednotky, optické zapisovací mechaniky) jsou zakázána.
- Příslušná rozhraní se používají jen na vybraných kontrolovaných pracovních stanicích.
- Přístupy ke všem serverům a síťovým zařízením a procesy na všech těchto zařízeních (firewally, routery), které jsou u zhotovitele používány pro účely elektronického přenosu dat, jsou neustále monitorovány a zaznamenávány do protokolu.
- Zálohovací pásky jsou uchovávány v ohnivzdorném trezoru, do něhož má přístup pouze oddělení IT.
- Přenos dat mezi jednotlivými místy probíhá přes VPN.

5. Kontrola vkládání údajů

Opatření na zajištění toho, aby bylo možno dodatečně prověřit a zjistit, zda a kým byly do systémů na zpracování dat vloženy osobní údaje a zda a kým byly tyto údaje změněny nebo odstraněny.

- Přihlašovací a systémové aktivity prováděné na všech pracovních stanicích a serverech jsou automaticky zaznamenávány do protokolu.
- Při shromažďování resp. evidenci údajů nelze získat přístup ke kompletním datovým souborům nebo k více než jednomu datovému souboru současně.
- U všech souborů jsou k dispozici srozumitelné údaje o přesném času a informace o uživateli.
- Všechny změny v systému pro shromažďování údajů jsou automaticky zaznamenávány do protokolu, a to s uvedením času a uživatele.
- Každý den se provádí zabezpečení všech údajů a protokolů s příslušnými informacemi o pořízení, změně nebo výmazu údajů.
- Záložní nosiče dat jsou uchovávány v trezoru.

6. Kontrola zpracování

Opatření na zajištění toho, aby byly osobní údaje, které se zpracovávají na základě pověření, zpracovávány pouze podle pokynů objednatele:

- Vymezení odpovědností mezi objednatelem a zhotovitelem je s ohledem na konkrétní pověření upraveno příslušnou smlouvou.
- Kontaktní osoby společnosti ThomasLloyd („vedoucí projektu“), které jsou uvedeny v příslušné smlouvě vztahující se k danému pověření, jsou oprávněny vydávat ostatním pracovníkům ThomasLloyd pokyny ohledně užívání a zpracování osobních údajů.
- Všichni pracovníci, kteří působí pro ThomasLloyd, jsou poučeni o dodržování ustanovení o ochraně údajů a jsou k tomuto dodržování smluvně zavázáni.
- Externí zadávání činností zaměřených na zpracování údajů je možné pouze na základě předchozího souhlasu příslušného objednatele, jestliže se jedná o údaje objednatele (zde vyloučeno); jsou uzavírány smlouvy o zpracování osobních údajů.
- Příprava dotazníku probíhá na základě vzájemné dohody s objednatelem; dotazník schvaluje objednatel.
- Programování probíhá podle schváleného dotazníku.
- Vedoucí projektu a pověřenec/pověřenci pro ochranu osobních údajů provádějí namátkovou kontrolu shody.

7. Kontrola dostupnosti

Opatření na zajištění ochrany osobních údajů před náhodným zničením nebo náhodnou ztrátou:

- Ochrana proti virům a malwaru, zabezpečení sítě bránou.
- Ochrana všech pracovních stanic a serverů proti výpadku.
- Zabezpečení diskových systémů proti výpadku (RAID).
- Synchronní kopírování na záložní systémy.
- Zajištění rychlé obnovy, včetně obnovy profilů uživatelů.
- Každodenní kompletní zabezpečení všech datových souborů a e-mailové komunikace.
- Každodenní zálohování prováděné pro všechny důležité servery, včetně systémového nastavení a tvorby protokolů.
- Ochrana záložních nosičů dat proti odcizení, zneužití a požáru formou jejich uložení v trezoru uvnitř kanceláře a mimo kancelář (jiná část budovy).
- K dispozici je zálohové napájení UPS.
- Zabezpečení před externím přístupem je zajištěno prostřednictvím dvouúrovňové koncepce firewallu, včetně systému detekce průniku (Intrusion Detection System - IDS) se softwarem od různých výrobců.
- Je prováděno dvojí antivirové testování pomocí softwaru od různých výrobců, přičemž aktualizace signatur probíhá několikrát denně.

8. Povinné oddělování údajů

Opatření na zajištění toho, aby byly osobní údaje, které byly shromážděny pro různé účely, zpracovávány odděleně:

- Údaje jsou v souladu s předpisy o ochraně osobních údajů povinně rozdělovány podle objednatelů a pověření.
- Z hlediska organizace se provádí rozlišení mezi vývojem programů, realizací programů, shromažďováním údajů a zpracováváním údajů a mezi ostatními firemními oblastmi.
- Kontrola organizace je popsána ve skupinových směrnících a přístupových právech.
- Údaje získané dotazováním a osobní údaje jsou fyzicky odděleny.
- Přístup je umožňován v souladu s koncepcí oprávnění.
- Po ukončení pověření se podle zadání příslušného objednatele provádí výmaz osobních údajů.