ZMLUVA O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

uzatvorená podľa čl. 28 ods. 3 všeobecného nariadenia o ochrane údajov (ďalej len „**GDPR**") medzi:

(I) **Univerzita Komenského v Bratislave**

so sídlom Šafárikovo nám. 6, 814 99 Bratislava 1, IČO: 00397865, konajúc prostredníctvom: prof. JUDr. Marek Števček, DrSc., rektor, kontaktné údaje zodpovednej osoby (DPO): dpo@uniba.sk (ďalej len „**Prevádzkovateľ**");

a

(II) **Dokumenta, a.s.**

so sídlom Strojnícka 103, 821 05 Bratislava, IČO: 35966726, konajúc prostredníctvom: Martin Mrázik, predseda predstavenstva a Andrea Pasztoriková, člen predstavenstva, kontaktné údaje zodpovednej osoby (DPO): andrea.pasztorikova@dokumenta.sk (ďalej len „**Sprostredkovateľ**");

Prevádzkovateľ a Sprostredkovateľ ďalej spoločne ako „**Zmluvné strany**" a každý samostatne ako „**Zmluvná strana**";

ZMLUVNÉ STRANY SA DOHODLI NA NASLEDOVNOM:

1.1 **Účel spracúvania**: Prevádzkovateľ týmto poveruje Sprostredkovateľa na spracúvanie osobných údajov na účely:

a. Právne a zmluvné účely, najmä pre potreby vnútorných administratívnych účelov;
b. Plnenie zákonných povinností;
c. Bezpečnosť osobných údajov a IT systémov;
d. Archívne účely;
e. Štatistické účely,

v mene Prevádzkovateľa, a to výlučne v súlade s touto zmluvou, GDPR a pokynmi Prevádzkovateľa, keďže na tieto účely sa spracúvajú osobné údaje prostredníctvom Automatizovaného systému elektronickej správy registratúry a obehu dokumentov pre Univerzitu Komenského v Bratislave, vrátane certifikovaného elektronického informačného systému na správu registratúry s kolobehom interných dokumentov „Document ManagementSystem" (ďalej len „**Systém**")

1.2 **Povaha a predmet spracúvania**: Povaha spracúvania je daná hlavnými zmluvnými vzťahmi medzi Zmluvnými stranami, ktoré sú upravené dvomi samostatnými zmluvami, a to:

a. Zmluvou o dielo (ďalej len „**Hlavná zmluva 1**");
b. Zmluvou o podpore prevádzky, údržbe a rozvoji informačného systému (ďalej len „**Hlavná zmluva 2**").

1.3 Spracúvanie bude zahŕňať akékoľvek spracovateľské operácie, ktoré sú nevyhnutne potrebné pre zabezpečenie prevádzkyschopnosti Systému, a to najmä podpora pri implementácii, testovaní a zabezpečovaní interoperability so všetkými informačnými systémami, ktoré sú integrované so Systémom ako aj pri poskytovaní všetkých služieb technickej podpory, prevádzky, údržby a rozvoja Systému tak ako sú definované v Hlavnej zmluve 2.

1.4 Spracúvanie bude zahŕňať akékoľvek spracovateľské operácie, ktoré sú nevyhnutne potrebné pre dodanie Systému a s tým spojenými službami Sprostredkovateľa na základe Hlavnej zmluvy 1 a Hlavnej zmluvy 2, a to najmä migrácia dát, vykonávanie bezpečnostného, funkčného a akceptačného testovania, údržby, prevádzky a rozvoja Systému a ďalších činností, ktoré by v zmysle Hlavnej zmluvy 1 a/alebo Hlavnej zmluvy 2 spôsobovali potrebu spracúvania osobných údajov.

1.5 **Doba spracúvania**: Počas trvania Hlavnej zmluvy 1 a Hlavnej zmluvy 2 alebo až do vydania pokynu Prevádzkovateľa adresovanému Sprostredkovateľovi o ukončení spracúvania osobných údajov k určitému dňu.

1.6 **Typ osobných údajov**: Prevádzkovateľ poveruje Sprostredkovateľa spracúvať také typy osobných údajov, ktoré sú nevyhnutné pre riadne poskytovanie jednotlivých služieb poskytovaných na základe Hlavnej zmluvy 1 a Hlavnej zmluvy 2.

1.7 Zmluvné strany sú povinné v prípade potreby zmien v rozsahu a typoch spracúvaných osobných údajov striktne dodržiavať základné zásady spracúvania osobných údajov podľa čl. 5 ods. 1 GDPR, a to najmä zásadu minimalizácie rozsahu spracúvania podľa čl. 5 ods. 1 písm. c) GDPR.

1.8 Nižšie Zmluvné strany vymedzili orientačný zoznam typov osobných údajov, ktoré bude Sprostredkovateľ oprávnený pri poskytovaní služieb podľa Hlavnej zmluvy 1 alebo Hlavnej zmluvy 2 spracúvať, tým však nie je dotknutý bod 1.6 tejto zmluvy, ak by počas trvania Hlavnej zmluvy 1 alebo Hlavnej zmluvy 2 nastala zmena v type spracúvaných osobných údajov.

a. **Právne a zmluvné účely, najmä vnútorné administratívne účely:**

Bežné kategórie osobných údajov: ÁNO, a to najmä:

- Osobné údaje zahrnuté do akýchkoľvek registratúrnych záznamov určených na interné zdieľanie medzi fakultami UK, rektorátom UK a samostatne hospodáriacimi súčasťami UK pre vnútorné administratívne potreby;

Osobitné kategórie osobných údajov: ÁNO, a to najmä:

- Osobné údaje týkajúce sa špecifických potrieb študentov (§ 100 Zákona o vysokých školách).

Údaje týkajúce sa uznania viny za trestné činy a priestupky: NIE (údaje týkajúce sa disciplinárnych previnení zamestnancov a študentov, či porušeniach ubytovacieho poriadku na internátoch nemajú charakter priestupkov).

Rodné čísla: ÁNO.

b. **Plnenie zákonných povinností:**

Bežné osobné údaje: ÁNO, a to najmä:

- Akékoľvek osobné údaje zahrnuté do registratúrnych záznamov, ktoré je Prevádzkovateľ povinný evidovať podľa č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o archívoch a registratúrach"; a to najmä:
    - Všetky došlé a odoslané záznamy v elektronickej i písomnej podobe, z ktorých je možné identifikovať pôvodcu registratúrneho záznamu, dátum jeho vzniku a ďalšie relevantné údaje, vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu registratúrneho záznamu;
    - Všetky Registratúrne záznamy, ktoré vytvoril Prevádzkovateľ ako pôvodca registratúry, vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu registratúrneho záznamu;
    - Všetky spisy ako súbory registratúrnych záznamov, ktoré sa týkajú jednej veci a ktoré vytvoril Prevádzkovateľ ako pôvodca registratúry, vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu registratúrneho záznamu;

Osobitné kategórie osobných údajov: ÁNO, ak sú zahrnuté do registatúrnych záznamov alebo archívnych dokumentov v súlade s čl. 9 ods. 2 GDPR.

Údaje týkajúce sa uznania viny za trestné činy a priestupky: NIE.

Rodné čísla: ÁNO.

c. **Archívne účely:**

Bežné osobné údaje: ÁNO, a to najmä:

- Akékoľvek osobné údaje zahrnuté do registratúrnych záznamov, ktoré je Prevádzkovateľ povinný evidovať podľa č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o archívoch a registratúrach"; a to najmä:

- Všetky došlé a odoslané záznamy v elektronickej i písomnej podobe, z ktorých je možné identifikovať pôvodcu registratúrneho záznamu, dátum jeho vzniku a ďalšie relevantné údaje, vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu registratúrneho záznamu;
- Všetky Registratúrne záznamy, ktoré vytvoril Prevádzkovateľ ako pôvodca registratúry, vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu registratúrneho záznamu;
- Všetky spisy ako súbory registratúrnych záznamov, ktoré sa týkajú jednej veci a ktoré vytvoril Prevádzkovateľ ako pôvodca registratúry, vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu registratúrneho záznamu;
- Archívne dokumenty, ktoré vytvoril Prevádzkovateľ ako pôvodca registratúry, ak majú trvalú dokumentárnu hodnotu vrátane akýchkoľvek osobných údajov umožňujúcich identifikovať dotknuté osoby figurujúce v obsahu archívneho dokumentu

- všetky archívne dokumenty, ktoré vznikli z činnosti pôvodcu registratúry.

Osobitná kategória údajov: ÁNO, ak sú zahrnuté do registatúrnych záznamov alebo archívnych dokumentov v súlade s čl. 9 ods. 2 GDPR.
Údaje týkajúce sa uznania viny za trestné činy a priestupky: NIE.
Rodné čísla: ÁNO.

d. **Bezpečnosť osobných údajov a IT systémov:**

Bežné osobné údaje: ÁNO, a to najmä:

- rôzne digitálne dáta a identifikátory, najmä logovacie záznamy, údaje s charakterom elektronických komunikačných metadát s identifikátorom umožňujúcim priamu alebo nepriamu identifikáciu dotknutej osoby (napr. IP adresa, MAC adresa, IMSEI zariadenia, IMSI zariadenia, typ prehliadača, typ operačného systému, poskytovateľa internetového pripojenia a pod.);
- prístupové heslá registrovaných používateľov Systému;
- prihlasovacie identity registrovaných používateľov Systému;
- prístupové role a oprávnenia priradené konkrétnym používateľom Systému;
- výsledky bezpečnostných a funkčných testov, vrátane osobných údajov osôb, ktoré ich vykonávali;
- akékoľvek osobné údaje zahrnuté do projektovej, technickej a bezpečnostnej dokumentácie viažucej sa ku systému;
- akékoľvek osobné údaje zahrnuté do dokumentácie a procesov riešenia bezpečnostných incidentov týkajúcich ;
- akékoľvek osobné údaje zahrnuté do žiadostí a vybavovania prevádzkových požiadaviek na servisnú a technickú podporu Systému.

Osobitná kategória údajov: NIE.
Údaje týkajúce sa uznania viny za trestné činy a priestupky: NIE.
Rodné čísla: NIE.

e. **Štatistické účely:**

Bežné identifikačné údaje: ÁNO, a to najmä:

- Iné bežné osobné údaje spracúvané na vyššie uvedené účely definované v bode 1.1 tejto zmluvy;

Osobitné kategórie osobných údajov: NIE.
Údaje týkajúce sa uznania viny za trestné činy a priestupky: NIE.
Rodné čísla: ÁNO.

1.9 <u>Kategórie dotknutých osôb</u>: Sprostredkovateľ je oprávnený spracúvať v mene Prevádzkovateľa pri poskytovaní služieb nevyhnutných na plnenie Hlavnej zmluvy 1 alebo Hlavnej zmluvy 2 identity a osobné údaje okruhov dotknutých osôb v nasledovnom rozsahu:

a.	Právne a zmluvné účely:	- Fyzické osoby zahrnuté do registratúrnych záznamov, spisov a archívnych dokumentov, ktoré je potrebné zdieľať v rámci UK v rámci interných administatívnych procesov.
b.	Archívne účely	- Fyzické osoby zahrnuté do registratúrnych záznamov, spisov a archívnych dokumentov.
c.	Bezpečnosť osobných údajov a IT systémov:	- Používatelia Systému s pridelenými prístupovými právami a rolami evidovaní v Systéme a fyzické osoby figurujúce v technickej, prevádzkovej a bezpečnostnej dokumentácii viažucej sa k Systému alebo inak súviacej s implementáciou, testovaním, údržbou a prevádzkou Systému.
d.	Plnenie zákonných povinností:	- fyzické osoby, ktorých osobné údaje spracúva Prevádzkovateľ na základe evidovania doručenej korešpondencie v príslušnom module Systému pri plnení povinnosti ustanovenej v § 16 ods. 2 písm. a) zákona č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov. - Akékoľvek iné fyzické osoby, ktorých osobné údaje bude potrebné spracúvať v Systéme pri plnení zákonných povinností Prevádzkovateľa
e.	Štatistické účely	- Akékoľvek okruhy dotknutých osôb, ktorých osobné údaje sú spracúvané na účely definované v tejto zmluve.

1.10 **Práva a povinnosti Zmluvných strán**:

a. **Zdokumentované pokyny**. Sprostredkovateľ spracúva osobné údaje len na základe zdokumentovaných pokynov Prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácie, s výnimkou prípadov, keď si to vyžaduje právo Únie alebo právo členského štátu, ktorému Sprostredkovateľ podlieha; v takom prípade Sprostredkovateľ oznámi Prevádzkovateľovi túto právnu požiadavku pred spracúvaním, pokiaľ dané právo takéto oznámenie nezakazuje zo závažných dôvodov verejného záujmu. Za zdokumentovaný pokyn sa považuje aj objednávka Prevádzkovateľa alebo inštrukcia emailom alebo ustanovenie Hlavnej zmluvy 1 alebo Hlavnej zmluvy 2, z ktorého vyplýva oprávnenie alebo povinnosť pre Sprostredkovateľa.

b. **Mlčanlivosť**. Sprostredkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch získaných od alebo v mene Prevádzkovateľa a zabezpečí, aby sa osoby oprávnené spracúvať osobné údaje (napr. jeho zamestnanci alebo ďalší sprostredkovatelia) zaviazali, že zachovajú dôvernosť / mlčanlivosť o spracúvaných osobných údajoch Prevádzkovateľa.

c. **Bezpečnosť osobných údajov**. Sprostredkovateľ prijal primerané bezpečnostné opatrenia podľa čl. 32 GDPR bližšie uvedené v prílohe č. 1 tejto zmluvy, ktoré boli Prevádzkovateľom detailnejšie preskúmané počas auditu pred uzatvorením tejto zmluvy.

e. **Súčinnosť.** Sprostredkovateľ je povinný pomáhať Prevádzkovateľovi pri plnení povinnosti Prevádzkovateľa reagovať na žiadosti o výkon práv dotknutej osoby a ďalších povinností Prevádzkovateľa podľa čl. 32 až 36 s prihliadnutím na povahu spracúvania a informácie dostupné Sprostredkovateľovi.

f. **Žiadosti dotknutých osôb.** Sprostredkovateľ nie je oprávnený sám odpovedať na žiadosti dotknutých osôb Prevádzkovateľa a akékoľvek žiadosti dotknutých osôb doručené Sprostredkovateľovi, ktoré sa týkajú Prevádzkovateľa, je Sprostredkovateľ okamžite povinný preposlať Prevádzkovateľovi. Sprostredkovateľ je povinný poskytovať súčinnosť Prevádzkovateľovi aj v prípade akéhokoľvek konania alebo sporu týkajúceho sa alebo súvisiaceho so spracúvaním osobných údajov podľa tejto zmluvy.

g. **Ukončenie.** Po ukončení poskytovania služieb týkajúcich sa spracúvania osobných údajov na základe ukončenia Hlavnej zmluvy 1, i.e. po odovzdaní Systému Prevádzkovateľovi budú vymazané alebo vrátané Prevádzkovateľovi akékoľvek osobné údaje, ktoré nebudú nevyhnutné pre poskytovanie služieb Sprostredkovateľa podľa Hlavnej zmluvy 2. Po ukončení Hlavnej zmluvy 2 a rozhodnutí Prevádzkovateľa Sprostredkovateľ všetky osobné údaje buď vymaže, anonymizuje alebo vráti Prevádzkovateľovi a vymaže všetky existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov.

h. **Porušenie ochrany osobných údajov.** Sprostredkovateľ je povinný bezodkladne (najneskôr do 48 hodín) oznámiť Prevádzkovateľovi každé opodstatnené podozrenie, že došlo k porušeniu ochrany osobných údajov.[1] Sprostredkovateľ nie je oprávnený oznamovať porušenie ochrany osobných údajov týkajúcich sa tejto zmluvy dozorným orgánom ani dotknutým osobám. Ak dôjde k porušeniu ochrany osobných údajov u Sprostredkovateľa, je Sprostredkovateľ povinný dané porušenie zdokumentovať podľa čl. 33 ods. 5 GDPR; dané zdokumentovanie Sprostredkovateľ poskytne Prevádzkovateľovi. Sprostredkovateľ nie je povinný oznamovať porušenia dotknutým osobám, za ktorých spracúvanie osobných údajov zodpovedá (ako prevádzkovateľ) Prevádzkovateľ.

ch. **Audity.** Sprostredkovateľ poskytne Prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností v čl. 28 GDPR a umožní audity, ako aj kontroly vykonávané Prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ, k ktorým prispieva. Prípadné náklady vzniknuté s výkonom auditu vrátane nákladov na poradcu Sprostredkovateľa a Prevádzkovateľa, ktorí sa budú zúčastňovať na audite znáša výlučne Prevádzkovateľ, pričom audity nesmú narúšať bežnú prevádzku Sprostredkovateľa a neprimerane ho obmedzovať.

i. **Vlastné účely.** Sprostredkovateľ nesmie osobné údaje spracúvané na základe tejto zmluvy spracúvať na svoje vlastné účely spracúvania osobných údajov, ak to nie je nevyhnutné pre splnenie Sprostredkovateľových vlastných zákonných povinností. Sprostredkovateľ sa zaväzuje spracúvané osobné údaje nepoužiť v rozpore s oprávnenými záujmami a očakávaniami dotknutých osôb, neohrozovať ani nepoškodzovať ich práva a právom chránené záujmy a svojím konaním nesmie neoprávnene zasahovať do práva na ochranu ich osobnosti a súkromia.

j. **Komunikácia.** Bez ohľadu na ustanovenia Hlavnej zmluvy 1 alebo Hlavnej zmluvy 2, akékoľvek otázky týkajúce sa tejto zmluvy a ochrany osobných údajov Zmluvné strany komunikujú prostredníctvom kontaktných údajov uvedených v záhlaví tejto zmluvy, a to vrátane emailovej komunikácie.

1.11 **Ďalší sprostredkovatelia.** Sprostredkovateľ je povinný dodržiavať podmienky zapojenia ďalšieho sprostredkovateľa podľa čl. 28 ods. 2 a 4 GDPR. Sprostredkovateľ zodpovedá za všetko spracúvanie osobných údajov ďalšími sprostredkovateľmi ako keby spracúval osobné údaje sám a zaväzuje sa zaviazať ďalších sprostredkovateľov tými istými podmienkami ako sú upravené v tejto zmluve. Zapojenie sub-sprostredkovateľa do spracúvania osobných údajov vykonávaného na základe tejto

[1] V zmysle čl. 4 bod 12 GDPR: *„porušenie ochrany osobných údajov" je porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim;*

zmluvy na strane Sprostredkovateľa podlieha predchádzajúcemu písomnému súhlasu Prevádzkovateľa.

1.12 **Ďalšie podmienky**. Zmluvné strany sa dohodli na ďalších podmienkach spracúvania nasledovne:

a. Sprostredkovateľ nebude získavať osobné údaje v mene Prevádzkovateľa;

b. Sprostredkovateľ nebude v mene Prevádzkovateľa plniť informačnú povinnosť podľa čl. 13/14 GDPR;

c. Sprostredkovateľ je v nevyhnutnej miere potrebnej na riadne poskytovanie služieb podľa Hlavnej zmluvy 1 oprávnený komunikovať s dotknutými osobami, čím nie je nijako dotknutá Sprostredkovateľova povinnosť podľa bodu 1.6 písm. f) tejto zmluvy.

1.13 **Záverečné ustanovenia**. Táto zmluva sa riadi a vykladá podľa slovenského práva a právomoc rozhodovať spory medzi týkajúce sa tejto zmluvy majú príslušné slovenské súdy. Táto zmluva je vyhotovená v dvoch rovnopisoch, pričom každá Zmluvná strana obdrží jeden rovnopis.

1.14 **Začiatok spracúvania osobných údajov:** Sprostredkovateľ je oprávnený začať spracúvať osobné údaje v mene Prevádzkovateľa v rozsahu a za podmienok podľa tejto zmluvy až na základe pozitívneho výsledku auditu, ktorý vykoná Prevádzkovateľ s cieľom objektívne preveriť Sprostredkovateľovu schopnosť dodržiavať povinnosti ustanovené v GDPR. Výsledok auditu uchováva zodpovedná osoba Prevádzkovateľa pre potreby kontroly Úradu na ochranu osobných údajov SR minimálne 3 roky po ukončení spolupráce Zmluvných strán.

1.15 **Rozväzovacia podmienka pre Hlavnú zmluvu 1 a Hlavnú zmluvu 2:** V prípade, ak Sprostredkovateľ neprejde cez audit Prevádzkovateľa v zmysle bodu 1.6 písm. ch) tejto zmluvy a bodu 1.10 tejto zmluvy z dôvodu fatálnych nedostatkov pri zabezpečovaní ochrany osobných údajov a tieto Sprostredkovateľ neodstráni ani na základe výzvy Prevádzkovateľa v primeranej lehote určenej Prevádzkovateľom, tak Prevádzkovateľ má právo odstúpiť od Hlavnej zmluvy 1 a Hlavnej zmluvy 2. Pre odstránenie pochybností platí, že fatálnym nedostatkom v zmysle predošlej vety sa rozumie: identifikácia vysokého rizika porušenia ochrany osobných údajov v dôsledku neprijatia, neuplatňovania alebo nesprávneho uplatňovania vhodných technických a organizačných bezpečnostných opatrení na strane Sprostredkovateľa, ktoré by boli zistené auditom Prevádzkovateľa vykonaným podľa 1.6 písm. ch) tejto zmluvy alebo podľa bodu 1.10 tejto zmluvy.

1.16 **Odkazy**. Akékoľvek odkazy na GDPR v tejto zmluve znamenajú odkazy na významovo obdobné alebo relevantné ustanovenie zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene alebo doplnení niektorých zákonov, alebo iného vnútroštátneho predpisu v oblasti ochrany osobných údajov, ak by sa mal takýto zákon alebo predpis vzťahovať na dané spracúvanie namiesto alebo popri GDPR, a naopak.

1.17 Táto zmluva nadobúda platnosť dňom jej podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv

PREVÁDZKOVATEĽ

V Bratislave dňa _____ 2026

Univerzita Komenského

prof. JUDr. Marek Števček, DrSc. rektor

SPROSTREDKOVATEĽ

Bratislave dňa

Dokumenta, a.s.

Martin Mrázik, predseda predstavenstva

Andrea Pasztoriková, člen predstavenstva

Príloha č. 1

Prijaté bezpečnostné opatrenia Sprostredkovateľa

Technické a organizačné opatrenia prijaté Sprostredkovateľom podľa čl. 32 GDPR:	Áno	Nie
Zabezpečenie objektu Sprostredkovateľa pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia)	☒	☐
Bezpečné uloženie fyzických nosičov osobných údajov (napr. uloženie listinných dokumentov v uzamykateľných skriniach alebo trezoroch)	☒	☐
Šifrová ochrana obsahu dátových nosičov a šifrová ochrana dát premiestňovaných prostredníctvom počítačových sietí	☒	☐
Prístup k informačným systémom len prostredníctvom hesiel	☒	☐
Detekcia prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete alebo z dátových nosičov	☒	☐
Používanie legálneho softvéru	☒	☐
Bezpečné vymazanie osobných údajov z dátových nosičov	☒	☐
Zariadenie na likvidáciu dátových nosičov osobných údajov napr. skartovač	☒	☐
Pravidelná aktualizácia operačného systému a programového aplikačného vybavenia	☒	☐
Interná politika ochrany osobných údajov	☒	☐
Interná politika IT bezpečnosti	☒	☐
Pseudonymizácia osobných údajov	☒	☐
Proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania	☒	☐
Ochrana pred nevyžiadanou elektronickou poštou (anti-spam)	☒	☐
Firewall	☒	☐
Pravidlá prístupu k internetu (napr. zamedzenie pripojenia k určitým webovým sídlam)	☒	☐
Logovanie	☒	☐
Test funkcionality dátového nosiča zálohy	☒	☐
Vytváranie záloh s vopred zvolenou periodicitou	☒	☐
Test obnovy informačného systému zo zálohy	☒	☐
Vymedzenie internej zodpovednosti za porušenie GDPR zamestnancami Sprostredkovateľa	☒	☐
Oboznámenie zamestnancov s prijatými internými politikami v oblasti ochrany osobných údajov	☒	☐
Vzdelávanie zamestnancov v oblasti ochrany osobných údajov a IT bezpečnosti	☒	☐

Vedenie zoznamu aktív a jeho aktualizácia	☒	☐
Kontrola vstupu do chránených priestorov Sprostredkovateľa	☒	☐
Prideľovanie prístupových práv a úrovní prístupu (rolí) zamestnancom	☒	☐
Správa hesiel	☒	☐
Vzájomné zastupovanie zamestnancov (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru)	☒	☐
Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, USB) mimo chránených priestorov a vymedzenie zodpovednosti	☒	☐
Pravidlá pre bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov	☒	☐
Postup pri riešení jednotlivých typov bezpečnostných incidentov	☒	☐
Postupy pri haváriách, poruchách a iných mimoriadnych situáciách	☒	☐
Vedenie záznamov o spracovateľských činnostiach podľa článku 30 ods. 2 GDPR	☒	☐
Vydanie poverenia a pokynov pre príjemcov údajov (čl. 32 ods. 4 a čl. 29 GDPR)	☐	☐
Poverenie zodpovednej osoby (*data protection officer*) u Sprostredkovateľa	☐	☐
Aplikovanie štandardných bezpečnostných opatrení v oblasti vývoja softvéru pre systémy využívané Prevádzkovateľom (napr. eSystém) tzv. SDLC (Software Development Life Cycle) opatrenia (viď nižšie konkrétnejšie)	☐	☐
Primerané SDLC opatrenia pôsobiace na systémy Prevádzkovateľa prijaté pre fázu plánovania, primárne: - Identifikácia a analýza bezpečnostných rizík Stanovenie bezpečnostných požiadaviek, ktoré musí eSystém spĺňať, pričom vždy musia primerane pokrývať aspekty ako je autentifikácia, autorizácia, šifrovanie, ochrana údajov a odolnosť voči útokom	☐	☐
Primerané SDLC opatrenia pôsobiace na systém Systém prijaté pre fázu analýzy a návrhu: - Primerané zabezpečenie IT bezpečnosti a kybernetickej odolnosti už od fázy návrhu softvérovej architektúry a komponentov - To zahŕňa najmä bezpečný návrh architektúry v rovine správneho oddelenie komponentov, minimalizácie prístupových bodov a implementácie bezpečnostných mechanizmov na úrovni architektúry. - Použitie osvedčených postupov a štandardov pre vývoj softvéru (napr. ENISA, OWASP Top 10, Sans TOP 25) - Používanie bezpečnostných vzorov (Security Patterns): Sprostredkovateľ bude aplikovať osvedčené bezpečnostné vzory pre riešenie bežných bezpečnostných problémov (napr. Input Validation, Output Encoding). - Analýza povrchu útoku (Attack Surface Analysis): Sprostredkovateľ identifikujte všetky potenciálne vstupné a výstupné body aplikácie, resp. systému, ktoré by mohli byť cieľom útoku, a navrhne vhodné opatrenia na ich zabezpečenie.	☐	☐

- Výber bezpečných technológií a knižníc: Sprostredkovateľ je povinný pri výbere technológií a knižníc vyberať tie, ktoré majú dobrú bezpečnostnú históriu a sú pravidelne aktualizované.		
Primerané SDLC opatrenia pôsobiace na systém Systém prijaté pre fázu implementácie, primárne: - Bezpečné kódovanie: Programátori dodržiavajú osvedčené postupy bezpečného kódovania, aby sa minimalizovali zraniteľnosti v kóde. Používajú sa nástroje na statickú analýzu kódu a penetračné testovanie na identifikáciu a opravu chýb. Cieľom je minimalizácia vzniku zraniteľností softvéru, ako sú SQL injection, cross-site scripting (XSS), buffer overflows, a ďalšie. - Statická analýza kódu (Static Application Security Testing - SAST): Sprostredkovateľ je povinný využívať nástroje na statickú analýzu kódu, ktoré automaticky kontrolujú zdrojový kód na prítomnosť potenciálnych zraniteľností a porušení bezpečnostných štandardov. - Peer review kódu: Sprostredkovateľ je povinný vykonávať aj revízie kódu inými, resp. viacerými kvalifikovanými vývojármi, ktorí môžu odhaliť potenciálne bezpečnostné problémy a chyby. - Riadenie konfigurácií: Implementuje sa proces riadenia konfigurácií, aby sa sledovali a kontrolovali všetky zmeny v softvérovom prostredí. - Používanie len bezpečných API a knižníc: Ak Sprostredkovateľ používa externé API alebo knižnice, je povinný kvalifikovane a s náležitou odbornou starostlivosťou overiť, že sú bezpečné a aktualizované a dôkladne sa oboznámiť so súvisiacou technickou a bezpečnostnou dokumentáciou pre optimálnu bezpečnostnú konfiguráciu danej API. - Validácia vstupov (Input Validation): Sprostredkovateľ je povinný dôsledne validovať všetky vstupy od používateľov a iných systémov, aby zabránil potenciálnym útokom prostredníctvom nevalidných dát – napr. formou kontroly nepovolených znakov potenciálne vedúce k útokom typu Cross-Site Scripting - XSS. - Správne spracovanie chýb a výnimiek: Sprostredkovateľ je povinný implementovať bezpečné mechanizmy na spracovanie chýb a výnimiek. - Používanie bezpečných autentifikačných a autorizačných mechanizmov: Sprostredkovateľ je povinný implementovať silné autentifikačné metódy (napr. viacfaktorovú autentifikáciu) a robustné autorizačné mechanizmy na riadenie prístupu k zdrojom. - Ochrana citlivých dát: Sprostredkovateľ je povinný šifrovať citlivé dáta používateľov (osobné údaje) počas prenosu (napr. pomocou HTTPS) aj počas uchovávania (napr. šifrovanie databázy – napr. AES 256bit).	☐	☐
Primerané SDLC opatrenia pôsobiace na systém Systém prijaté pre fázu testovania, primárne: - Funkčné testovanie nasadzovanej zmeny: Sprostredkovateľ preveruje, či nasadenie zmien a novej verzie Systém bude v súlade s požiadavkami a pokynmi Prevádzkovateľa, ako aj či ich nasadenie v Prevádzkovateľom produkčnom prostredí systému Systém nemôže spôsobiť porušenie integrity, dostupnosti	☐	☐

alebo dôvernosti spracúvaných osobných údajov. Uvedené realizuje Sprostredkovateľ súhrnom funkčných testov, a to najmä:

- Unit testy: Testovanie jednotlivých komponentov alebo modulov systému.
- Integračné testy: Testovanie interakcií medzi rôznymi komponentmi systému.
- Systémové testy: Komplexné testovanie celého systému ako celku.
- Akceptačné testy (User Acceptance Testing - UAT): Testovanie z pohľadu koncového používateľa (Prevádzkovateľa) na overenie, či systém spĺňa jeho potreby.
- Regresné testy: Zabezpečenie toho, že nasadenie nových zmien neovplyvnilo existujúcu funkčnosť systému

- Testovanie bezpečnosti: Okrem funkčného testovania sa vykonáva aj komplexné testovanie bezpečnosti, aby sa odhalili a opravili bezpečnostné chyby a zraniteľnosti. Používajú sa rôzne metódy testovania bezpečnosti, ako napríklad penetračné testovanie a skenovanie zraniteľností. Okrem týchto testov bude Sprostredkovateľ realizovať nasledovné bezpečnostné testovanie:
  - Statická analýza kódu (SAST): Analýza zdrojového kódu na odhalenie potenciálnych bezpečnostných chýb ešte pred nasadením.
  - Dynamická analýza kódu (DAST): Testovanie bežiacej aplikácie z pohľadu útočníka.
  - Interactive Application Security Testing (IAST): Kombinácia statickej a dynamickej analýzy.
  - Fuzzing: Automatické generovanie veľkého množstva náhodných a neštandardných vstupov na odhalenie chýb a zraniteľností.
  - Testovanie autorizácie a autentifikácie: Dôkladné overenie, či prístup k osobným údajom a citlivým funkciám je správne riadený.
  - Testovanie spracovania chýb a výnimiek: Overenie, či systém pri chybách neprezrádza citlivé informácie.
  - Testovanie konfigurácie zabezpečenia: Kontrola, či sú správne nastavené bezpečnostné konfigurácie serverov, aplikácií a databáz.
- Dôkazy o vykonaných testoch: Sprostredkovateľ je povinný zdokumentovať výsledky testov a tieto uchovávať počas trvania Zmluvy.
- Odborná kvalifikácia testerov a vhodné nástroje: Sprostredkovateľ je povinný zabezpečiť, aby testovanie bezpečnosti vykonávali kvalifikovaní odborníci s použitím vhodných nástrojov.
- Pravidelnosť bezpečnostného testovania: Sprostredkovateľ je povinný vykonávať bezpečnostné testy nielen jednorazovo pri nasadení zmien, ale aj pravidelne (napríklad periodicky najmenej raz ročne alebo po každej významnej zmene systému).

- Zohľadnenie výsledkov threat modelingu: Sprostredkovateľ je povinný bezpečnostné testy cieliť primárne voči hrozbám a rizikám identifikovaným v predchádzajúcich fázach SDLC (napríklad pri modelovaní hrozieb). - Proces riešenia nájdených zraniteľností: Sprostredkovateľ je povinný mať definované postupy na riešenie a opravu nájdených bezpečnostných zraniteľností, vrátane ich prioritizácie a overenia po oprave.		
Primerané SDLC opatrenia pôsobiace na Systém prijaté pre fázu nasadenia a údržby: - Bezpečná konfigurácia prostredia: Sprostredkovateľ bude spolupracovať s Prevádzkovateľom do tej miery, aby sa softvér Systému nasadzoval do bezpečného prostredia s adekvátnymi bezpečnostnými kontrolami, ako sú firewally, systémy detekcie narušenia a riešenia na správu identít a prístupov (napr. IAM). - Bezpečnostný hardening: Sprostredkovateľ je povinný implementovať postupy pre "hardening" operačných systémov, serverov a aplikácií (napr. odstránenie nepotrebných služieb, zmena predvolených hesiel, obmedzenie prístupových práv). - Segmentácia siete: Sprostredkovateľ je povinný vývoj a testovanie realizovať v rámci vlastnej segmentovanej počítačovej siete, aby sa v prípade prelomenia jedného segmentu obmedzil dopad na ostatné časti infraštruktúry. - Bezpečná konfigurácia samotnej aplikácie Systém: Sprostredkovateľ je povinný zabezpečiť, že aj samotná aplikácia Systém je správne a bezpečne nakonfigurovaná (napr. nastavenie silných hesiel pre administrátorské účty, zabezpečenie komunikačných kanálov). - Pravidelné aktualizácie a opravy: Sprostredkovateľ bude zabezpečovať, aby softvér systému Systém bol pravidelne aktualizovaný o najnovšie bezpečnostné záplaty a opravy chýb. Sprostredkovateľ implementuje proces na riadenie zraniteľností a odstraňovanie identifikovaných chýb. - Testovanie záplat pred nasadením: Sprostredkovateľ uplatňuje proces testovania bezpečnostných záplat v testovacom prostredí pred ich nasadením do produkčného prostredia, aby sa predišlo nežiaducim vplyvom na funkčnosť systému Systém. - Monitorovanie a reakcia na incidenty: Sprostredkovateľ implementuje proces na monitorovanie bezpečnostných incidentov a na rýchlu a efektívnu reakciu určenú na ich maximálnu možnú mitigáciu, pričom v prípade vzniku porušenia ochrany osobných údajov následkom bezpečnostného incidentu bezodkladne po zistení tohto porušenia ihneď informuje zodpovednú osobu Prevádzkovateľa.	☐	☐