

ZMLUVA O SPRACÚVANÍ OSOBNÝCH ÚDAJOV

dalej označovaná len ako **Zmluva** je uzavretá medzi nasledovnými zmluvnými stranami:

(1) **Národná koalícia pre digitálne zručnosti a povolania Slovenskej republiky**

záujmové združenie právnických osôb so sídlom Bottova 7939/2A, 811 09 Bratislava – Staré Mesto, Slovenská republika, IČO: 52 828 123, zapísané v Registri záujmových združení právnických osôb vedenom Okresným úradom Bratislava s registračným číslom OUBAOVVS12019/140232, email:

(Digitálna koalícia alebo Prevádzkovateľ)

a

(2) **SHL Talent Assessment s.r.o.**

so sídlom Poličanská 1487, Újezd nad Lesy, 190 16 Praha 9, Česká republika, IČO: 07562861, zapísaná v Městský soud v Praze, oddíl C, vložka 303152, za ktorú samostatne koná PhDr. Tomáš Rodný, Country Manager, na základe plné moci, e-mail:

(Partner alebo Sprostredkovateľ)

uzavretá najmä podľa ustanovení

- a) článku 28 odseku 3 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (**GDPR**)
- b) a tiež v súlade s ustanoveniami ďalších platných právnych predpisov Slovenskej republiky a platných právnych aktov Európskej únie.

s nasledovným obsahom:

PREAMBULA

- A. Partner a združenie Digitálna koalícia spolu 4.10.2024 uzavreli Rámcovú dohodu (**Hlavná zmluva**), predmetom ktorej je poskytnutie a integrácia psychometrického nástroja na posúdenie kompetencií jednotlivca a odporúčanie relevantných zhlukov povolání. Plnenie Hlavnej zmluvy sa týka realizácie projektu **Digitálny radca: Poradenstvo v kontexte meniaceho sa trhu práce v IT**, ktorý realizuje Digitálna koalícia (**Projekt**).
- B. Partner bude pri plnení Hlavnej zmluvy spracúvať informácie týkajúce sa identifikovaných alebo identifikovateľných fyzických osôb (**Dotknutá osoba**). Tieto informácie predstavujú osobné údaje v zmysle GDPR (**Osobné údaje**).
- C. S ohľadom na takéto nastavenie vzťahov je združenie Digitálna koalícia v zmysle GDPR prevádzkovateľom a Partner je sprostredkovateľom.
- D. Podľa ustanovení článku 28 ods. 3 GDPR sa spracúvanie osobných údajov sprostredkovateľom musí riadiť zmluvou, ktorá bude sprostredkovateľa zaväzovať voči prevádzkovateľovi a ktorou sa stanoví predmet a doba spracúvania, povaha a účel spracúvania, typ spracúvaných osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa.

Berúc do úvahy vyššie uvedené sa Prevádzkovateľ a Sprostredkovateľ dohodli na nasledovných zmluvných podmienkach.

ČLÁNOK 1: ÚVODNÉ USTANOVENIA A PREHLÁSENIA STRÁN

- 1.1. Spracúvanie osobných údajov podľa Zmluvy sa riadi najmä GDPR, v niektorých špecifických prípadoch sa spracúvanie môže riadiť aj ustanoveniami zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (**Zákon o ochrane osobných údajov**; spoločne s GDPR **Predpisy na ochranu osobných údajov**).
- 1.2. Sprostredkovateľ prehlasuje, že je oprávnený uzavrieť Zmluvu a plniť povinnosti v nej uvedené. Sprostredkovateľ tiež vyhlasuje a ubezpečuje Prevádzkovateľa, že prijal dostatočné technické a organizačné opatrenia a poskytuje dostatočné záruky, aby spracúvanie osobných údajov spĺňalo požiadavky Predpisov na ochranu osobných údajov, aby bola zabezpečená ochrana práv Dotknutých osôb.
- 1.3. Prevádzkovateľ prehlasuje, že je oprávnený uzavrieť a plniť Zmluvu a poveriť Sprostredkovateľa spracovaním osobných údajov za podmienok dohodnutých v Zmluve.

ČLÁNOK 2: PREDMET A ÚČEL ZMLUVY

- 2.1. **[Predmet Zmluvy]** Predmetom Zmluvy je poverenie Sprostredkovateľa Prevádzkovateľom na spracúvanie osobných údajov Dotknutých osôb na účely určené v Zmluve, v rozsahu a za podmienok špecifikovaných v Zmluve a prijatie poverenia Sprostredkovateľom.
- 2.2. **[Účel Zmluvy]** Účelom Zmluvy je úprava vzájomných práv a povinností zmluvných strán pri spracúvaní osobných údajov Dotknutých osôb Sprostredkovateľom v mene Prevádzkovateľa tak, aby spracúvanie prebiehalo v súlade s Predpismi na ochranu osobných údajov a aby bola zaistená dostatočná a účinná ochrana spracúvaných osobných údajov.
- 2.3. **[Poverenie]** Združenie Digitálna koalícia ako prevádzkovateľ touto Zmluvou poveruje Partnera ako sprostredkovateľa spracúvaním osobných údajov v mene združenia Digitálna koalícia.

ČLÁNOK 3: SPRACÚVANÉ OSOBNÉ ÚDAJE

- 3.1. **[Účel spracúvania osobných údajov]** Účelom spracúvania osobných údajov je výhradne plnenie Hlavnej zmluvy. Bez predchádzajúceho písomného súhlasu Prevádzkovateľa nie je Sprostredkovateľ oprávnený spracúvať osobné údaje na žiadne iné účely.
- 3.2. **[Miesto spracúvania osobných údajov]** Zmluvné strany sa dohodli, že miestom spracúvania osobných údajov bude sídlo Sprostredkovateľa. Spracúvanie osobných údajov Sprostredkovateľom na inom mieste je možné len na základe predchádzajúceho písomného súhlasu Prevádzkovateľa.
- 3.3. **[Typ osobných údajov]** Prevádzkovateľ poskytne Sprostredkovateľovi nasledovné osobné údaje:
 - a) **identifikačné údaje žiadateľa o účasť v Projekte:** meno, priezvisko, prípadne tituly, dátum narodenia a vek;
 - b) **kontaktné údaje žiadateľa o účasť v Projekte:** telefónne číslo a emailová adresa;
 - c) **údaje o zamestnaní žiadateľa o účasť v Projekte:**
 - údaj o tom, či je žiadateľ evidovaný ako Uchádzač o zamestnanie alebo Záujemca o zamestnanie a údaje o jeho súčasnej a minulých pracovných pozíciách;
 - akékoľvek iné osobné údaje, ktoré o sebe žiadateľ o účasť v Projekte poskytne;
 - údaj o návšteve internetového portálu Projektu a údaje o podaní žiadosti o účasť v Projekte.
 - po overení splnenia podmienok cieľovej skupiny (Zájemcovia o zamestnanie alebo Uchádzači o zamestnanie) okrem vyššie uvedených údajov aj nasledovné kategórie osobných údajov:
 - d) **údaje osobného charakteru účastníka Projektu:** údaje vyplývajúce z psychometrických testov, podľa ktorých sa určí profil Záujemcu o zamestnanie alebo Uchádzača o zamestnanie v relácii na vhodné zhluky povolání (napríklad silné stránky žiadateľa a pod.);

- e) **údaje účastníka Projektu o účasti v Projekte:** údaj o tom, či sa Záujemca o zamestnanie alebo Uchádzač o zamestnanie zúčastnil psychometrického testovania, ak je to relevantné, tiež výstupné správy z testovania pre analytické účely a účely vykázania účasti na Projekte.
- 3.4. **[Kategórie spracúvaných osobných údajov]** Osobné údaje, ktoré Digitálna koalícia poskytne Sprostredkovateľovi sú všeobecnými osobnými údajmi. Sprostredkovateľ nemá právo spracúvať osobitné kategórie osobných údajov v zmysle ustanovení § 16 Zákona o ochrane osobných údajov a Článku 9 GDPR.
- 3.5. **[Kategórie dotknutých osôb]** Dotknutými osobami sú účastníci Projektu.
- 3.6. **[Doba spracúvania osobných údajov]** Spracúvateľ je oprávnený spracúvať osobné údaje v mene Digitálnej koalície od dátumu účinnosti Zmluvy až do ukončenia trvania Hlavnej zmluvy, ak z pokynov Prevádzkovateľa alebo právnych predpisov nevyplýva kratšia doba.
- 3.7. **[Povaha spracúvania osobných údajov]** Spracúvateľ má právo osobné údaje, ktoré spracúva:
- a) získať a zaznamenať;
 - b) usporadúvať, uchovávať a archivovať;
 - c) prehliadať, opravovať, aktualizovať;
 - d) spracúvať ich automatizovanými aj neautomatizovanými prostriedkami spracúvania; spracúvanie automatizovanými prostriedkami bude Sprostredkovateľ vykonávať v internom systéme Digitálnej koalície;
 - e) spracúvať inými spracovateľskými operáciami povolenými právnymi predpismi;
 - f) vymazať a zlikvidovať.

ČLÁNOK 4: PODMIENKY SPRACÚVANIA OSOBNÝCH ÚDAJOV

- 4.1. **[Spracúvané údaje]** Sprostredkovateľ bude spracúvať osobné údaje (i) poskytnuté Sprostredkovateľovi Prevádzkovateľom v súvislosti s Hlavnou zmluvou a za účelom jej plnenia, (ii) získané Sprostredkovateľom pri plnení Hlavnej zmluvy alebo (iii) poskytnuté Sprostredkovateľovi priamo či nepriamo zo strany Dotknutej osoby, a to výhradne v rozsahu nevyhnutnom pre naplnenie účelu spracúvania podľa Zmluvy.
- 4.2. **[Základné podmienky spracúvania]** Sprostredkovateľ sa zaväzuje spracúvať osobné údaje iba na základe pokynov Prevádzkovateľa, a podľa podmienok upravených v Zmluve a zaväzuje sa dodržiavať záruky v nej uvedené.
- 4.3. **[Pokyny Prevádzkovateľa]** Prevádzkovateľ zodpovedá za pokyny udelené Sprostredkovateľovi vo vzťahu k spracúvaniu osobných údajov; to nezbavuje Sprostredkovateľa povinnosti informovať Prevádzkovateľa, ak podľa jeho názoru konkrétny pokyn porušuje Predpisy na ochranu osobných údajov. V takomto prípade Sprostredkovateľ do vykonania nápravy vykoná len také operácie s osobnými údajmi, ktoré neznesú odklad. Ak si vykonanie pokynov Prevádzkovateľa vyžiada vznik dodatočných nákladov na strane Sprostredkovateľa v súvislosti s vykonaním týchto pokynov, je Sprostredkovateľ oprávnený požadovať úhradu vzniknutých nákladov, pokiaľ predmetné úkony nie sú súčasťou odmeny podľa Hlavnej zmluvy.
- 4.4. **[Práva a povinnosti Prevádzkovateľa]** Prevádzkovateľ je:
- a) povinný spracúvať osobné údaje v súlade s Predpismi na ochranu osobných údajov;
 - b) oprávnený zadať Sprostredkovateľovi písomné pokyny týkajúce sa spracúvania osobných údajov;

- c) povinný pravidelne aktualizovať údaje o spracúvaných osobných údajoch uvedené v Článku 3 Zmluvy.

4.5. **[Základné povinnosti Sprostredkovateľa]** Sprostredkovateľ je povinný:

- a) poskytovať Prevádzkovateľovi akúkoľvek súčinnosť v rozsahu potrebnom na plnenie účelu Zmluvy a Hlavnej zmluvy a všetky informácie nevyhnutné na preukázanie súladu s povinnosťami Sprostredkovateľa vyplývajúcimi zo Zmluvy a z Predpisov na ochranu osobných údajov;
- b) spracúvať osobné údaje v súlade s príslušnými právnymi predpismi, a to najmä s Predpismi na ochranu osobných údajov, a to len počas doby spracúvania určenej podľa Zmluvy;
- c) oznámiť (a sprístupniť) svojim zamestnancom podmienky ochrany osobných údajov, ktorých aktuálna verzia sa nachádza na webovej stránke www.digitalnyradca.sk;
- d) pomáhať Prevádzkovateľovi pri zabezpečení plnenia povinností podľa GDPR s prihliadnutím na povahu spracúvania a informácie dostupné Sprostredkovateľovi;
- e) Sprostredkovateľ je (so zohľadnením povahy spracúvania) povinný v čo najväčšej miere pomáhať Prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení svojich povinností reagovať na žiadosti o výkon práv dotknutej osoby podľa Kapitoly III GDPR.

4.6. **[Spracúvanie v súlade s účelom]** Sprostredkovateľ je povinný nevyužívať a nezdržovať osobné údaje na iné účely, než na účely určené v Zmluve alebo v Hlavnej zmluve, teda:

- a) spracúvať osobné údaje výhradne na účely podľa Zmluvy alebo Hlavnej zmluvy;
- b) spracúvať výhradne také osobné údaje, ktoré rozsahom a obsahom zodpovedajú určenému účelu a sú nevyhnutné pre jeho dosiahnutie;
- c) udržiavať údaje získané na rozdielne účely oddelene a zabezpečiť, aby osobné údaje boli spracúvané iba spôsobom, ktorý zodpovedá účelu, pre ktorý boli zhromaždené;
- d) spracúvať iba správne, kompletné a aktuálne osobné údaje vo vzťahu k účelu ich spracúvania a s nesprávnymi a nekompletnými údajmi naložiť v súlade s Predpismi na ochranu osobných údajov;
- e) spracúvať osobné údaje tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu práva na zachovanie ľudskej dôstojnosti;
- f) nezískavať osobné údaje od Dotknutých osôb pod zámienkou iného účelu alebo inej činnosti;
- g) spracúvať osobné údaje v súlade s dobrými mravmi a konať spôsobom, ktorý nie je v rozpore s právnymi predpismi.

4.7. **[Vybavovanie podnetov Dotknutých osôb]** Ak Sprostredkovateľ dostane žiadosť alebo podnet od Dotknutej osoby v súvislosti so spracúvaním osobných údajov podľa Zmluvy, je povinný túto žiadosť alebo podnet bezodkladne predložiť Prevádzkovateľovi a poskytnúť Prevádzkovateľovi súčinnosť pri plnení povinností vo vzťahu k žiadostiam a podnetom Dotknutých osôb.

4.8. **[Ukončenie spracúvania]** Po ukončení spracúvania osobných údajov je Sprostredkovateľ povinný všetky osobné údaje vymazať alebo vrátiť Prevádzkovateľovi a vymazať všetky existujúce kópie osobných údajov, ak uchovávanie týchto údajov nevyžadujú právne predpisy.

4.9. **[Preukázanie plnenia povinností a umožnenie auditov]** Sprostredkovateľ je povinný poskytnúť Prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností podľa článku 28 GDPR a umožniť vykonanie auditov alebo kontrol vykonávaných Prevádzkovateľom alebo ním povereným audиторom a prispievať k nim; zároveň je povinný umožniť Úradu na ochranu osobných údajov SR kontrolu dodržiavania pravidiel ochrany osobných údajov a dodržiavania predmetu Zmluvy.

- 4.10. **[Výnimky z riadenia sa Zmluvou a pokynmi]** Sprostredkovateľ spracúva osobné údaje len na základe Hlavnej zmluvy alebo zdokumentovaných písomných pokynov Prevádzkovateľa, a to aj pokiaľ ide o prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, s výnimkou prípadov, keď si to vyžaduje právo Európskej 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.
- 4.11. **[Oznámenie porušení]** Sprostredkovateľ je povinný bezodkladne písomne informovať Prevádzkovateľa, ak sú podľa jeho názoru porušované Predpisy na ochranu osobných údajov alebo iné relevantné právne predpisy, a to aj v prípade, ak ide o porušenie zo strany Prevádzkovateľa alebo ak je pokyn Prevádzkovateľa v rozpore s Predpismi na ochranu osobných údajov podľa ustanovení odseku 4.3. Zmluvy.
- 4.12. **[Orgány verejnej moci]** Zmluva nebráni Sprostredkovateľovi spracúvať osobné údaje takým spôsobom, ktorý vyžaduje zákon, nariadenie alebo príslušný súd, či dozorný orgán. Ak dozorný orgán alebo príslušný súd vydá žiadosť týkajúcu sa spracúvania osobných údajov, vrátane žiadosti o obmedzenie spracovávaní, výmaz, opravu osobných údajov, poskytnutie informácií alebo vykonanie akýchkoľvek iných opatrení, je Sprostredkovateľ povinný bez zbytočného odkladu informovať Prevádzkovateľa o doručení akejkoľvek takej žiadosti pred tým, ako na túto žiadosť zareaguje alebo vykoná iný úkon týkajúci sa spracovávaných osobných údajov, alebo čo najskôr, ako je možné legitímne očakávať, ak akýkoľvek zákon alebo nariadenie predpisuje Sprostredkovateľovi okamžitú odpoveď dozornému orgánu alebo príslušnému súdu s výnimkou prípadu, že také oznámenie Prevádzkovateľovi je zakázané zákonom, nariadením alebo rozhodnutím či príkazom.
- 4.13. **[Oznámenie kontroly]** Sprostredkovateľ je povinný bezodkladne oznámiť Prevádzkovateľovi zahájenie či vykonanie kontroly či vyšetrovanie zo strany Úradu pre ochranu osobných údajov SR alebo iného dozorného orgánu a poskytovať Prevádzkovateľovi podrobné informácie o priebehu takej kontroly, ako aj o prípadných nadväzujúcich správnych či súdnych konaní. Ak Úrad pre ochranu osobných údajov SR alebo iný dozorný orgán zahájí kontrolu či vyšetrovanie Prevádzkovateľa, je Sprostredkovateľ povinný poskytovať Prevádzkovateľovi pri tejto kontrole všetku potrebnú súčinnosť.

ČLÁNOK 5: ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV

- 5.1. **[Technické a organizačné opatrenia]** Sprostredkovateľ je povinný prijať a zabezpečiť dodržiavanie príslušných technických a organizačných opatrení podľa ustanovení § 39 Zákona o ochrane osobných údajov a Článku 32 GDPR, ktoré zodpovedajú spracúvaným údajom a pri zohľadnení druhu spracúvania a poskytnutých informácií bude Prevádzkovateľa podporovať pri dodržiavaní povinností uvedených v ustanoveniach § 39, § 40 a § 41 Zákona o ochrane osobných údajov alebo zodpovedajúcich ustanoveniach GDPR. Sprostredkovateľ je povinný pravidelne testovať, posudzovať a hodnotiť efektivitu svojich prijatých opatrení. Sprostredkovateľ sa zaväzuje dodržiavať technické a organizačné opatrenia uvedené v Prílohe č. 1 Zmluvy. V prípade potreby Sprostredkovateľ vykoná ďalšie vhodné opatrenia na zaistenie zodpovedajúcej a vhodnej úrovne zabezpečenia osobných údajov (s ohľadom na stav techniky, náklady, povahu, rozsah, kontext, účely a riziká vykonávaného spracúvania, okrem iného najmä vo vzťahu k opatreniam vyžadovaným smernicou Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) a predpismi, ktorými bude táto smernica transponovaná do právneho poriadku Slovenskej republiky. Sprostredkovateľ sa zaväzuje dodržiavať samostatne alebo spoločne so sub-sprostredkovateľmi technické a organizačné opatrenia uvedené v Prílohe č. 1 Zmluvy. Ak je povinnosť uložená Sprostredkovateľovi podľa Prílohy č. 1 k Zmluve, namiesto Sprostredkovateľa ju môžu plniť len sub-sprostredkovatelia.

- 5.2. **[Zameranie opatrení]** Prijaté technické a organizačné opatrenia sú zamerané najmä na:
- a) pseudonymizáciu a šifrovanie osobných údajov;
 - b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;
 - c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu;
 - d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.
- 5.3. **[Zabezpečenie osobných údajov]** Sprostredkovateľ je povinný chrániť osobné údaje pred ich poškodením, zničením, stratou zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmkoľvek inými neprípustnými spôsobmi spracúvania; na tento účel je Sprostredkovateľ povinný prijať primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracovania osobných údajov v jednotlivých účeloch spracúvania a to formou a za podmienok stanovených Predpismi na ochranu osobných údajov, pričom vezme do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.
- 5.4. **[Porušenie bezpečnosti]** V prípade porušenia bezpečnosti osobných údajov podľa ustanovení predchádzajúceho odseku je Sprostredkovateľ povinný bezodkladne prijať primerané nápravné opatrenia ihneď, ako je to možné a poskytnúť Prevádzkovateľovi všetky relevantné informácie, o ktoré ho v tejto súvislosti požiada a potrebnú súčinnosť za účelom odstránenia následkov porušenia bezpečnosti osobných údajov.
- 5.5. **[Mlčanlivosť a dôvernosť]** Sprostredkovateľ je povinný zachovávať mlčanlivosť o všetkých osobných údajoch, s ktorými príde do styku. Povinnosťou mlčanlivosti musí Sprostredkovateľ zaviazat' aj všetkých svojich zamestnancov, prípadne iné osoby, ktoré prídu do styku s osobnými údajmi; tie nesmie využiť ani pre svoju potrebu, ani ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť bez predchádzajúceho písomného súhlasu Prevádzkovateľa, okrem prípadov, ak poskytnutie alebo sprístupnenie osobných údajov je nevyhnutné na zabezpečenie spracúvania osobných údajov podľa tejto Zmluvy alebo povinnosť poskytnutia alebo sprístupnenia osobných údajov vyplýva z osobitných právnych predpisov alebo z rozhodnutia orgánu verejnej moci. Túto mlčanlivosť je Sprostredkovateľ povinný zachovávať aj po skončení poverenia podľa Zmluvy a je povinný viesť evidenciu o akomkoľvek vykonanom sprístupnení alebo poskytnutí osobných údajov podľa predchádzajúcej vety, a to po celú dobu trvania Zmluvy.

ČLÁNOK 6: SPÔSOB SPRACÚVANIA OSOBNÝCH ÚDAJOV

- 6.1. **[Spracúvanie v elektronickej podobe]** Sprostredkovateľ bude osobné údaje spracúvať v elektronickej podobe pomocou prostriedkov informačných technológií.
- 6.2. **[Základné zásady zabezpečenia]** Pri spracúvaní osobných údajov Sprostredkovateľ prijme a bude dodržiavať najmä tieto zásady zabezpečenia osobných údajov:
- a) elektronické dáta obsahujúce osobné údaje budú ukladané a ďalej spracúvané výhradne na nosičoch (napr. prenosných či neprenosných dátových nosičoch, sieťových dátových úložiskách), ktoré sú v majetku či v oprávnenom užívaní Prevádzkovateľa alebo Sprostredkovateľa;
 - b) osobné údaje nebudú združované s osobnými údajmi spracovávanými Sprostredkovateľom pre iné účely alebo pre iných prevádzkovateľov. Bez predchádzajúceho písomného pokynu Prevádzkovateľa nebudú osobné údaje združované s osobnými údajmi spracovávanými pre tretie osoby;

- c) prístup k osobným údajom majú iba príslušné oprávnené osoby s využitím individuálnych prístupových údajov, a to v rozsahu zodpovedajúcom oprávneniam príslušnej oprávnenej osoby;
 - d) pri spracovaní osobných údajov budú zhotovované elektronické záznamy, ktoré umožnia určiť, kedy, kým a z akého dôvodu boli osobné údaje spracované;
 - e) nosiče osobných údajov budú zabezpečené a chránené pred neoprávneným prístupom.
- 6.3. **[Dokumentácia]** Sprostredkovateľ je povinný dokumentovať technické a organizačné opatrenia prijaté na ochranu osobných údajov, pravidelne túto dokumentáciu aktualizovať a na vyžiadanie ju predložiť Prevádzkovateľovi ku kontrole. Sprostredkovateľ tiež predloží Prevádzkovateľovi všetky správy dokumentujúce bezpečnostné audity vykonané Sprostredkovateľom alebo Sprostredkovateľom určeným audítorom. Sprostredkovateľ umožní audity a inšpekcie vykonávané Prevádzkovateľom alebo iným audítorom k prevereniu zabezpečenia osobných údajov, a to po predchádzajúcom oznámení zo strany Prevádzkovateľa.
- 6.4. **[Spracúvanie len v rámci EÚ/EHP]** Sprostredkovateľ môže spracúvať osobné údaje na svojich informačných systémoch, ako aj informačných systémoch tretích osôb výlučne v rámci EÚ/EHP. Ak by malo dochádzať k cezhraničnému spracúvaniu osobných údajov, je Sprostredkovateľ povinný vyžiadať si súhlas Prevádzkovateľa s cezhraničným spracúvaním.
- 6.5. **[Audit]** Prevádzkovateľ alebo ním menovaný uznávaný nezávislý audítor je kedykoľvek počas trvania Zmluvy oprávnený vykonávať audity a inšpekcie v zariadeniach Sprostredkovateľa a jeho sub-sprostredkovateľov v súlade so Zmluvou. Akýkoľvek audit u Sprostredkovateľa je obmedzený len na posúdenie dodržiavania povinností podľa Zmluvy a nebude sa vzťahovať na prístup k akýmkoľvek údajom iných prevádzkovateľov alebo údajom, ktoré súvisia s používaním bezpečnostných opatrení Sprostredkovateľa. Pri výkone kontroly alebo auditu je Sprostredkovateľ povinný vytvoriť primerané podmienky a bezodkladne poskytovať nevyhnutnú súčinnosť. Ak sú kontrola alebo audit realizované Prevádzkovateľom alebo ním poverenou osobou, je Prevádzkovateľ povinný Sprostredkovateľovi písomne oznámiť termín vykonania kontroly alebo auditu aspoň dva dni pred jeho začatím.
- 6.6. **[Bezpečnostný incident]** Sprostredkovateľ je povinný predchádzať porušeniu zabezpečenia osobných údajov. V prípade porušenia bezpečnostných opatrení vedúcich k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému zverejneniu alebo sprístupneniu osobných údajov (**Bezpečnostný incident**) je Sprostredkovateľ povinný **bezodkladne (najneskôr do 48 hodín)** odkedy sa o Bezpečnostnom incidente dozvedel, informovať o Bezpečnostnom incidente Prevádzkovateľa.
- 6.7. **[Oznámenie Bezpečnostného incidentu]** Oznámenie o porušení zabezpečenia osobných údajov musí obsahovať minimálne (i) opis povahy Bezpečnostného incidentu vrátane kategórií a približného počtu Dotknutých osôb a kategórií a približného počtu dotknutých záznamov o osobných údajoch, ako aj (ii) opis pravdepodobných dôsledkov porušenia ochrany osobných údajov a (iii) opis prijatých opatrení za účelom riešenia Bezpečnostného incidentu a zníženia možných negatívnych účinkov porušenia ochrany osobných údajov. Ak v dôsledku Bezpečnostného incidentu hrozí aj porušenie Zmluvy na strane Sprostredkovateľa, bude súčasťou oznámenia aj (iv) informácia o tomto porušení. Ak nie je možné poskytnúť všetky tieto informácie súčasne, môžu byť poskytované aj vo fázach vždy však bez zbytočného odkladu.
- 6.8. **[Dokumentácia Bezpečnostného incidentu]** Sprostredkovateľ je povinný zdokumentovať všetky Bezpečnostné incidenty a sprístupniť túto dokumentáciu Prevádzkovateľovi na základe jeho žiadosti.
- 6.9. **[Riešenie Bezpečnostného incidentu]** Po zistení Bezpečnostného incidentu je Sprostredkovateľ povinný podniknúť nevyhnutné a potrebné kroky za účelom zabezpečenia ochrany osobných údajov, ako aj za účelom obmedzenia akéhokoľvek možného negatívneho vplyvu na Dotknuté osoby. Sprostredkovateľ bude s Prevádzkovateľom spolupracovať pri reakcii na zistené Bezpečnostné incidenty.

- 6.10. **[Sub-sprostredkovatelia]** Sprostredkovateľ je oprávnený použiť na spracúvanie osobných údajov Dotknutých osôb podľa Zmluvy ako ďalšieho sprostredkovateľa osoby uvedené v Prílohe č. 2 Zmluvy. Iné osoby je Sprostredkovateľ oprávnený použiť iba na základe predchádzajúceho osobitného písomného povolenia Prevádzkovateľa. Sprostredkovateľ sprístupní Prevádzkovateľovi aktuálny zoznam sub-sprostredkovateľov (Prílohu č. 2 Zmluvy), ktorý zahŕňa názvy a sídla sub-sprostredkovateľov, ako aj rozsah služieb poskytovaných Sprostredkovateľovi. Prevádzkovateľ súhlasí s využívaním uvedených sub-sprostredkovateľov na uvedený rozsah služieb.
- 6.11. **[Nastavenie vzťahov so sub-sprostredkovateľmi]** Sprostredkovateľ je povinný pravidelne monitorovať činnosť sub-sprostredkovateľov a je zodpovedný za spracovanie osobných údajov sub-sprostredkovateľmi rovnako ako keby údaje spracúval priamo on. Sprostredkovateľ je zároveň povinný so sub-sprostredkovateľmi uzavrieť zmluvu, v ktorej im uloží rovnaké alebo prísnejšie povinnosti ochrany osobných údajov, aké má on sám podľa Zmluvy. Sprostredkovateľ zodpovedá za to, že (i) každý ďalší sprostredkovateľ sa písomne zaviazal k povinnosti mlčanlivosti, alebo že sa na neho vzťahuje zákonná povinnosť mlčanlivosti a že (ii) každý ďalší sprostredkovateľ plní riadne svoje povinnosti v oblasti ochrany osobných údajov.

ČLÁNOK 7: ZODPOVEDNOSŤ SPROSTREDKOVATEĽA A SANKCIE

- 7.1. **[Náhrada škody a ujmy]** Sprostredkovateľ nesie zodpovednosť za ujmu vzniknutú Prevádzkovateľovi alebo Dotknutej osobe, ak (i) nesplnil povinnosti podľa Zmluvy, (ii) nesplnil povinnosti konkrétne stanovené pre Sprostredkovateľa Predpismi na ochranu osobných údajov alebo iným všeobecne záväzným právnym predpisom, alebo (iii) konal nad rámec či v rozpore s pokynmi Prevádzkovateľa podľa Zmluvy. V prípade vzniku škody alebo ujmy sa Sprostredkovateľ zaväzuje nahradiť Prevádzkovateľovi alebo Dotknutej osobe vzniknutú škodu alebo odčiniť nemajetkovú ujmu primeraným zadosťučinením, a to bezodkladne po výzve Prevádzkovateľa, najneskôr však 10 pracovných dní od doručenia výzvy.
- 7.2. **[Zmluvná pokuta]** Ak Sprostredkovateľ poruší ktorúkoľvek z povinností podľa Článku 4, Článku 5, Článku 6 a Článku 8 Zmluvy, má Prevádzkovateľ nárok na zaplatenie zmluvnej pokuty vo výške 5.000 EUR za každé jednotlivé porušenie ktorejkoľvek z týchto povinností (samostatne). Sprostredkovateľ je povinný zmluvnú pokutu zaplatiť do troch dní po doručení výzvy Prevádzkovateľa na jej zaplatenie. Zaplatením zmluvnej pokuty nie je dotknuté právo Prevádzkovateľa požadovať od Sprostredkovateľa popri zmluvnej pokute aj náhradu škody alebo nemajetkovej ujmy, a to aj vo výške prevyšujúcej dohodnutú zmluvnú pokutu.

ČLÁNOK 8: DÔVERNOSŤ

- 8.1. Spracúvanie osobných údajov má dôvernú povahu. Zmluvné strany sú povinné zachovávať mlčanlivosť o všetkých dôverných informáciách, ktoré im boli poskytnuté, alebo ktoré inak získali v súvislosti so Zmluvou alebo s ktorými sa oboznámili počas plnenia Zmluvy, resp. ktoré súvisia s predmetom jej plnenia, a to aj po ukončení účinnosti Zmluvy, s výnimkou nasledujúcich prípadov:
- a) ak je poskytnutie informácie vyžadované od dotknutej zmluvnej strany právnymi predpismi;
 - b) ak je informácia verejne dostupná z iného dôvodu ako je porušenie povinnosti mlčanlivosti dotknutou zmluvnou stranou;
 - c) ak ide o informácie, ktoré sa stanú po podpise Zmluvy verejne známymi, alebo ktoré možno po tomto dni získať z bežne dostupných informačných prostriedkov;
 - d) ak je informácia poskytnutá odborným poradcom dotknutej zmluvnej strany (vrátane právnych, účtovných, daňových a iných poradcov), ktorí sú buď viazaní všeobecnou profesionálnou povinnosťou mlčanlivosti, alebo ak sa voči dotknutej zmluvnej strane zaviazali povinnosťou mlčanlivosti;
 - e) ak je informácia vyžadovaná pre účely akéhokoľvek súdneho, rozhodcovského, správneho alebo iného konania, ktorého je dotknutá zmluvná strana účastníkom;
 - f) ak je informácia poskytnutá so súhlasom druhej zmluvnej strany.

- 8.2. Zmluvné strany sa zaväzujú, že dôverné informácie bez predchádzajúceho písomného súhlasu druhej zmluvnej strany nepoužijú pre seba alebo pre tretie osoby, neposkytnú tretím osobám a ani neumožnia prístup tretích osôb k nim. Za tretie osoby sa nepokladajú členovia orgánov zmluvných strán, audítori alebo právni poradcovia zmluvných strán, ktorí sú ohľadne im sprístupnených informácií viazaní povinnosťou mlčanlivosti na základe všeobecne záväzných právnych predpisov.

ČLÁNOK 9: KOMUNIKÁCIA

- 9.1. **[Spôsoby komunikácie]** Pokiaľ nie je v Zmluve uvedené inak, akékoľvek oznámenia, žiadosti a iné dokumenty alebo informácie určené druhej zmluvnej strane alebo vyžadované Zmluvou a akákoľvek iná komunikácia medzi zmluvnými stranami bude v slovenskom jazyku a bude doručená druhej zmluvnej strane jedným z nasledovných spôsobov:
- a) e-mailom na adresu druhej zmluvnej strany uvedenú v Zmluve (ak je to možné, tak s požiadavkou na oznámenie o doručení);
 - b) doporučenou poštou s doručenkou; alebo
 - c) kuriérskou službou, ktorá umožňuje overenie doručenia.
- 9.2. **[Doručenie]** Správa zaslaná vyššie uvedeným spôsobom sa považuje za doručенú druhej zmluvnej strane, ktorá je adresátom:
- a) v prípade doručenia e-mailom dňom prijatia potvrdenia o úspešnom doručení e-mailovej správy (alebo rovnocenného dokladu), alebo ak správa nebola odoslaná s požiadavkou na oznámenie o doručení, uplynutím nasledujúceho dňa po odoslaní správy;
 - b) v prípade doručenia poštou dňom prevzatia správy; ak zmluvná strana, ktorá je adresátom správy neprevezme alebo odmietne prevziať, alebo jej z iných dôvodov nie je možné správu doručiť, považuje sa správa za doručенú uplynutím desiateho pracovného dňa po odoslaní správy;
 - c) v prípade doručenia kuriérskou službou dňom prevzatia správy; ak zmluvná strana, ktorá je adresátom správy neprevezme alebo odmietne prevziať, alebo jej z iných dôvodov nie je možné správu doručiť, považuje sa správa za doručенú uplynutím desiateho pracovného dňa po odovzdaní správy kuriérskej službe.

ČLÁNOK 10: ZÁVEREČNÉ USTANOVENIA

- 10.1. **[Platnosť a účinnosť]** Zmluva nadobúda platnosť a účinnosť dňom jej podpisu obomi zmluvnými stranami (alebo poslednou z nich); ak právne predpisy ustanovujú povinné zverejnenie Zmluvy, je Zmluva účinná dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.
- 10.2. **[Trvanie Zmluvy]** Zmluva sa uzatvára na dobu spracúvania osobných údajov Sprostredkovateľom podľa ustanovení Článku 3 odseku 3.6. Zmluvy a zanikne splnením povinnosti Sprostredkovateľa uvedenej v Článku 4 odseku 4.8. Zmluvy.
- 10.3. **[Prílohy]** Neoddeliteľnou súčasťou Zmluvy sú aj jej prílohy:
- Príloha č. 1:** Technické a organizačné opatrenia na zabezpečenie ochrany osobných údajov;
- Príloha č. 2:** Zoznam ďalších sprostredkovateľov a príjemcov.
- 10.4. **[Vzdanie sa práva a oddeliteľnosť]** Vzdanie sa práva z porušenia akejkoľvek povinnosti podľa Zmluvy ktoroukoľvek zo zmluvných strán nie je vzdaním sa práva vyplývajúceho z ďalšieho porušenia tejto povinnosti, ani vzdaním sa práva vyplývajúceho z porušenia inej povinnosti podľa Zmluvy, ani tak nemôže byť interpretované. Neuplatnenie akéhokoľvek práva, ako aj omeškanie s jeho uplatnením nie je vzdaním sa práva, ani tak nemôže byť interpretované. Ak je ktorékoľvek z ustanovení Zmluvy neplatné, neúčinné alebo nevymáhateľné, alebo ak sa takým stane v budúcnosti, ostatné ustanovenia Zmluvy tým nebudú

dotknuté a zostanú platné, účinné a vykonateľné v plnom rozsahu podľa právnych predpisov. Zmluvné strany sa týmto zaväzujú nahradiť neplatné, neúčinné alebo nevykonateľné ustanovenia novými, ktoré budú svojim významom čo najbližšie významu ustanovení, ktoré sa stali neplatnými, neúčinnými alebo nevykonateľnými.

- 10.5. **[Jazyk a rovnopisy]** Zmluva je vyhotovená a podpísaná v slovenskom jazyku, v dvoch (2) rovnopisoch, pričom každá zmluvná strana si ponechá jeden (1) z rovnopisov.
- 10.6. **[Zmena Zmluvy]** Zmluva môže byť zmenená alebo doplnená len písomnými riadne očíslovanými dodatkami podpísanými oboma zmluvnými stranami.
- 10.7. **[Rozhodné právo]** Zmluva a jej výklad sa riadi právnym poriadkom Slovenskej republiky a platnými právnymi aktmi Európskej únie a bude interpretovaná najmä v súlade s GDPR alebo Zákonom o ochrane osobných údajov. Rovnaké pravidlá sa aplikujú aj na prílohy a dodatky Zmluvy a všetky mimozmluvné záväzky súvisiace so Zmluvou alebo z nej vyplývajúce.
- 10.8. **[Riešenie sporov]** Zmluvné strany sa dohodli, že akékoľvek spory, ktoré vzniknú zo Zmluvy, vrátane sporov o jej platnosť, výklad alebo ukončenie, budú prednostne riešené zmierom a v dobrej viere. Spory medzi Zmluvnými stranami, ktoré nebudú urovnané podľa predchádzajúcej vety, sa s konečnou platnosťou vyriešia na vecne a miestne príslušnom súde v Slovenskej republike.
- 10.9. **[Nahradenie predchádzajúcich dohôd]** Zmluva so všetkými jej ustanoveniami a prílohami predstavuje úplnú dohodu zmluvných strán o predmete Zmluvy a nahrádza všetky predchádzajúce rokovania a písomné alebo ústne dohody medzi zmluvnými stranami týkajúce sa predmetu Zmluvy.
- 10.10. **[Záverečné prehlásenia]** Zmluvné strany spoločne prehlasujú, že majú všetky potrebné profesionálne skúsenosti, odborné znalosti a zdroje potrebné na plnenie Zmluvy a ich finančná situácia umožňuje v dobrej viere prevziať záväzky uvedené v Zmluve. Zmluvné strany tiež spoločne prehlasujú, že si text Zmluvy prečítali, v plnom rozsahu porozumeli jej obsahu, ktorý je pre nich dostatočne určitý a vyjadruje ich slobodnú a vážnu vôľu prostú akýchkoľvek omylov, a že ju neuzatvárajú v tiesni a ani za nápadne nevýhodných podmienok pre ktorúkoľvek z nich, na znak čoho ju vlastnoručne podpisujú.

Podpisy strán

V Bratislave dňa 5.11.2024

Za Prevádzkovateľa

Za Sprostredkovateľa

Ing. Mário Lelovský, predseda predsedníctva

PhDr. Tomáš Rodný, Country Manager

PRÍLOHA Č. 1: TECHNICKE A ORGANIZAČNÉ OPATRENIA NA ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV



Security & Compliance - GDPR

SHL exists to help our clients win by providing deep people insights to inform talent decisions. As the global leader in assessment science, we help organizations and their leaders address the most pressing talent priorities by providing an unparalleled view of their workforce. Our unrivalled assessment service, benchmark data, extensive and analytic technology enable companies to influence genuine organizational change and drive tangible business outcomes from having the right people in the right roles at the right time.

DATA PROTECTION

In light of recent changes to data protection laws in the European Union, namely the introduction of the General Data Protection Regulation (GDPR) on 25th May 2018, SHL undertook multiple actions in furtherance of our compliance measures and as part of our on-going commitment to providing our clients' market leading security and data management.

1. Appointment of a Data Protection Officer (DPO)

SHL recognises itself as a data processor. Our core activities consist of the processing of personal data on behalf of our clients, the data controllers, which requires systematic, large-scale monitoring. Our processing may also include the processing of special categories of personal data on behalf of our data controller where stipulated.

SHL's Global Data Protection Officer (DPO) was designated on the basis of professional qualities including expert knowledge and qualification in data protection law and practices. If you require further information regarding the DPO please email DPO@SHL.com

2. Policies & Notices

SHL periodically conducts systematic updates of its external and internal facing privacy policies and notices. We have established a GDPR resources section on our [SHL.com](https://www.shl.com) website. The page includes a series of resources addressing SHL's approach and notices as part of our data protection compliance: the [SHL GDPR Whitepaper](#), [On-Demand Webinar](#), Data Protection Notices for [Candidate Support](#) and [Online Training Services](#), and a [Frequently Asked Questions](#) page. Clients are able to register to be notified automatically when any of these documents are updated.

In order to properly inform data subjects of the uses of their personal data and the lawful grounds which apply, each SHL platform and point of capture of personal data (as controller and processor) receive Data Protection Notices, which are periodically updated as required.

Policies are updated and/or introduced for the improvement of lawfulness, transparency, limitation, minimisation, accuracy, storage and security of personal data where necessary for the GDPR and other country specific legislation or interpretations. Updates include, but are not limited to, the Data Protection Policy, Information Security Policy, Data Retention Policy, End-User and System Use Policy, and Incident Response Plan.

3. Monitoring & Management

The SHL Global DPO heads a cross-department SHL Data Protection Working Party where relevant individuals meet with the DPO on a regular basis. In addition to an Information Security Officer, SHL also employs a Data Governance Specialist to support and monitor data protection requirements across the organisation. Additionally, key employees across SHL Legal and IT departments receive regular education and have data protection qualifications as part of the overall compliance program.

SHL conducts multiple Privacy Impact Assessments and Data Protection Impact Assessments (DPIAs) each year and employs outside technical and legal consultancy prior to the enactment of any proposed changes to the processing activities of personal data. The DPIAs form and inform internal data governance framework updates outlining regularly scheduled analysis and updates of data protection practices. Where the need for a DPIA is identified an SHL DPIA template is used, developed from the [guidelines](#) supplied by Article 29 Working Party/European Data Protection Board.

SHL manages a Record of Processing Activities (RoPA) for the appropriate management and awareness of personal data uses throughout the organisation, which maintains a record of how data processing changes as the organisation or internal business activities change. This is used to measure and maintain compliance and to understand how the use cases change as each business function develops.

SHL maintains the technical and organisational monitoring of systems, processes and third-parties with a relevant and relative schedule of analysis taking into account the nature, scope and context of the processing activities of the personal data. These include but are not limited to, data loss prevention, email monitoring and investigative functionality, CRM, Financial and marketing systems.

SHL has maintains a Privacy Information Management System (PIMS) for the management of all data protection matters within SHL.

4. Processes & Procedures

Where possible, procedural documents for uses of personal data within individual tasks (e.g. recruitment), have been developed to assist individuals who take a role within an activity, but would not be recognised as data processing activity owner so they are able to understand their data protection responsibility during such tasks.

Data subject rights, breach logging & reporting, employee training and data retention periods have one or more policy aligned to each area and undergo scheduled and/or ad hoc review and enhancement for ongoing improvement to data protection practices.

SHL conducts ongoing processes of technical and physical discovery and destruction of personal data where personal data is: a) no longer required for use; b) no longer required for further legal basis for retention or storage; c) duplicated; d) over captured, where purposes have changed and the data is no longer required on

the basis it was first captured. Retention and destruction procedural guidelines are in place for this and also continues to go under periodic review and evaluation.

5. Security

We prioritise data security: We understand and have always taken our security obligations seriously, long before the GDPR. Our commitment to security is demonstrated by our on-going certification programs that have been in place for many years. In particular, we have developed and implemented an ISO 27001 certified Information Security Management System for over 10 years running. Additionally, we have obtained ISO 22301 certification for our Business Continuity Practices and we have ISO 20000 certifications for our ability to professionally maintain, support and manage our IT services using best practices. Further information can be found [here](#).

SHL maintains annual compliance training for all employees and relevant contractors. This training includes data protection practices and cyber security, as well as specialised modules for IT and development staff on data handling further demonstrating the commitment to data protection.

6. Data Deletion

SHL acts as the data processor and only deletes data on the request of the data controller. SHL has a defined data deletion process and has an SLA of 30 days from once the deletion is approved by the client for the deletion to be completed.

7. Complying with International Transfer Rules

In accordance with our current practice we will continue to ensure we do not transfer data outside of the EEA without an appropriate data transfer structure in place. Currently, we have EU Standard Contractual Clauses ("Model Clauses") in effect for transfers outside of the EEA to ensure adequate levels of protection as permitted by the European Commission. We are also updating our policies and procedures in anticipation of the withdrawal of the United Kingdom from the European Union. Regardless of the outcome of Brexit, SHL is still committed to the GDPR and we are currently evaluating possible options with respect to the transfer of data between the UK and the EEA. We rely on self-certification under the EU-US Privacy Shield for transfers to the US. Privacy Shield is a selfcertification programme under which organisations can register with and confirm they meet specific privacy requirements.

The Privacy Shield is not expressly referenced in the GDPR, but it is recognised by the European Commission as providing adequate protection. We will continue to monitor any proposed changes to Privacy Shield and Model Clauses following the GDPR and ensure we upgrade our agreements and Privacy Shield certification as required.

8. Examples of Compliance with GDPR Articles

Article 13: The right to be informed

Our assessment platform includes a data protection notice which individuals are presented with prior to taking the assessment. This notice provides information to the individual about the collection and processing that we perform, in accordance with data protection legislation requirements.

As the assessment makes up one part of an overall recruitment process, (and the assessment is generally not your first point of candidate data collection) the Article 13 notice requirements may also need to be satisfied earlier than our assessment platform. You may employ several different methods, such as your careers website, an online application form, or applicant tracking system to receive initial applications, and collect other personal information e.g. CV or résumé information, residential address etc. In each of these systems, a data protection notice that addresses the full recruitment cycle would be required at the point of data collection.

You would need to seek independent legal advice on your compliance obligations under Article 13 GDPR.

Article 15 – 18: The right; of access, to rectification, to erase or to restrict processing

A candidate's request to access, correct, delete or restrict processing of data should be directed to you, as the data controller. We occasionally receive requests directly from candidates to delete their information, or to provide access to their assessment results. We redirect these candidate requests back to as the data controller. We then provide support and information to you as you require to meet your obligation to the candidate.

If we receive such a request directly from you as our client, we already have processes in place to carry out that request, whether that is promptly responding to a data subject access request, or a request for deletion of data. Clients often ask "how long do you retain data?" As a data processor, we retain data in accordance with our client agreements, meaning we delete data following a request from you, our clients. As part of our GDPR compliance strategy we made improvements within our platform to build in increased automation and efficiencies into our data deletion processes.

Article 20 The right to data portability

The right to data portability only applies:

- to personal data an individual (i.e. a candidate) has provided to our clients as the data controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means (it does not apply to paper records).

Given the context of the products and services that we offer, we see this right as being quite closely related to the right to access as noted above and we would direct any such requests back to you as the data controller, and then assist in your decisions to comply.

The information that is collected directly from the individual is limited, and therefore providing this in a "structured, commonly used, machine-readable and interoperable format" can be easily done on a case by case basis. It would be up to you as the data controller to determine the extent of the information that you would make available under this right.

Article 21 - The right to object

A candidate may have a right to object to the processing of their personal data if you, as the data controller, rely on legitimate interests as the legal basis for processing. Candidates are free to choose whether to take an assessment or not. If they object to the processing of data, an individual can simply close out of the assessment and we will not perform any further processing.

If the candidate objects after they have started an assessment, this will become a right to deletion under Article 15

Article 22 Rights in relation to automated decision making and profiling

The GDPR provides a right for individuals not to be subject to any automated decisions unless certain exemptions apply. Our clients often use our services to aid in making decisions as to whether to offer employment or a promotion to an individual. Our best practice guidelines recommend that our assessments should be used as part of an overall evaluation and should not be relied upon as the sole basis for any employment related decisions. For any other use of our assessments we would advise you to seek independent legal advice on your compliance obligations under Article 22 GDPR.

As the data controller, if you inform us you intend to use our assessment as part of an automated decision, we can follow your instructions regarding your approach to any permitted exception, such as sufficient notification to individuals that they may be subject to an automated decision.

9. Continual Improvement

SHL is committed to the continual improvement of its data protection activities. Each improvement is logged so patterns can be understood, and further areas of analysis can be identified.

If you are aware of any areas which can be improved in SHL's data protection activities, please do send an email outlining your suggestion clearly to DPO@SHL.com.

If you have any further questions, please either speak to your account manager or email data.questions@shl.com.

PRÍLOHA Č. 2: ZOZNAM ĎALŠÍCH SPROSTREDKOVATEĽOV A PRÍJEMCOV

Zoznam ďalších sprostredkovateľov				
Názov	IČO	Sídlo	Poskytované služby	Krajina
42 Organisational Assessments SRL	J40/305/2011 EUID: ROONRC.J40/305/2011	29A, Icoanei St., Bucharest 2, Rumunsko	spracovanie testových dát	Rumunsko
SHL Group Limited	01328744	1 Atwell Place, Thames Ditton Surrey KT7 0NE Veľká Británia	spracovanie testových dát	Veľká Británia

[Pokiaľ Sprostredkovateľ ku dňu podpisu Zmluvy nepoužíva žiadneho ďalšieho sprostredkovateľa, Príloha č. 2 bude ponechaná prázdna]