Podmínky zpracování osobních údajů

ve vztahu k službám

platné od 30. dubna 2025, verze 1.0

ODDÍL I

Článek 1
Účel a působnost

(a) Účelem těchto Podmínek zpracování osobních údajů (dále jen "Podmínky") je zajistit soulad s ustanovením článku 28 odst. 3 a 4 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

(b) Olympus Czech Group, s.r.o., člen koncernu, se sídlem Evropská 176/16, 160 41 Praha 6 a zpracovatel (zpracovatel) a správce se dohodli na těchto Podmínkách, aby zajistili soulad s ustanovením článku 28 odst. 3 a 4 nařízení (EU) 2016/679 a/nebo článku 29 odst. 3 a 4 nařízení (EU) 2018/1725.

(c) Tyto Podmínky se použijí na zpracování osobních údajů, jak je uvedeno v Příloze 1.

(d) Příloha I až III jsou nedílnou součástí těchto Podmínek.

(e) Těmito Podmínkami nejsou dotčeny povinnosti, které správce musí plnit na základě nařízení (EU) 2016/679 a/nebo nařízením (EU) 2018/1725.

(f) Tyto Podmínky, samy o sobě nezajišťují soulad s povinnostmi týkajícími se mezinárodního předávání podle kapitoly V. nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

Článek 2
Výklad

(a) V případech, kdy tyto Podmínky používají pojmy definované v nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725, mají tyto pojmy stejný význam jako v uvedeném nařízení.

(b) Tyto Podmínky jsou chápány a vykládány v souladu s ustanoveními nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.

(c) Tyto Podmínky nesmí být vykládány způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679 / nařízení (EU) 2018/1725, nebo který by omezoval základní práva nebo svobody subjektů osobních údajů.

ODDÍL II – POVINNOSTI STRAN

Článek 3
Popis zpracování

Podrobnosti týkající se operací zpracování, zejména kategorie osobních údajů a účely zpracování, pro něž jsou osobní údaje zpracovávány jménem správce, jsou uvedeny v příloze I.

Článek 4
Povinnosti stran

4.1. Pokyny

(a) Zpracovatel zpracovává osobní údaje pouze na základě písemně doložených pokynů správce, pokud mu takové zpracování neukládá právo Evropské unie nebo členského státu, které se na správce vztahuje. V tomto případě zpracovatel správce informuje o uvedeném právním požadavku před zpracováním, pokud to právní předpisy nezakazují z důvodů důležitého

veřejného zájmu. Po celou dobu zpracování osobních údajů může správce rovněž vydávat další pokyny. Tyto pokyny musí být vždy písemně doloženy.

(b) Zpracovatel neprodleně informuje správce v případě, že podle jeho názoru pokyny správce porušují nařízení (EU) 2016/679 / nařízení (EU) 2018/1725 nebo příslušné předpisy Evropské unie nebo členského státu o ochraně osobních údajů.

4.2. Omezení účelu

Zpracovatel zpracovává osobní údaje pouze pro konkrétní účel nebo účely zpracování, jak je stanoveno v příloze I, pokud od správce neobdrží další pokyny.

4.3. Doba trvání zpracování osobních údajů

Zpracování zpracovatelem probíhá pouze po dobu stanovenou v příloze I.

4.4. Zabezpečení zpracování

(a) Za účelem zajištění bezpečnosti osobních údajů musí zpracovatel zavést přinejmenším technická a organizační opatření uvedená v příloze II. Součástí těchto opatření musí být ochrana osobních údajů před narušením bezpečnosti, které by vedlo k jejich náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému zpřístupnění nebo přístupu k nim (porušení zabezpečení osobních údajů). Při posuzování vhodné úrovně zabezpečení vezmou strany v úvahu aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování a rizika pro subjekty osobních údajů.

(b) Zpracovatel poskytne svým zaměstnancům přístup ke zpracovávaným osobním údajům pouze v rozsahu nezbytně nutném pro provádění, správu a kontrolu smlouvy. Zpracovatel zajistí, aby se osoby oprávněné zpracovávat obdržené osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

4.5. Ciltivé údaje

Pokud zpracování zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu nebo o sexuálním životě či sexuální orientaci dané osoby nebo údaje týkající se odsouzení v trestních věcech a trestných činů (dále jen „citlivé údaje“), uplatní zpracovatel zvláštní omezení nebo další záruky.

4.6. Dokumentace a soulad

(a) Strany musí být schopny prokázat dodržování těchto Podmínek.

(b) Zpracovatel neprodleně a odpovídajícím způsobem zodpoví dotazy správce, které se týkají zpracovávání podle těchto Podmínek.

c) Zpracovatel poskytne správci veškeré informace potřebné k prokázání souladu s povinnostmi stanovenými v těchto Podmínkách, které vyplývají přímo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725. Zpracovatel též na žádost správce umožní audity činností zpracování, na něž se tyto Podmínky vztahují, a k těmto auditům přispěje, a to v přiměřených intervalech nebo pokud existují známky nesouladu. Při rozhodování o přezkumu nebo auditu může správce zohlednit příslušná osvědčení držená zpracovatelem.

(d) Správce se může rozhodnout, zda audit provede sám, nebo jím pověří nezávislého auditora. Audity mohou rovněž zahrnovat kontroly v objektech a prostorách zařízení zpracovatele a případně jsou předem včas ohlášeny.

(e) Strany na požádání zpřístupní informace uvedené v těchto Podmínkách, včetně výsledků případných auditů, příslušnému dozorovému orgánu, respektive příslušným dozorovým orgánům.

4.7. Využívání dílčích zpracovatelů osobních údajů

(a) Zpracovatel má obecné povolení správce k zapojení dílčích zpracovatelů ze schváleného seznamu uvedeného v příloze III. Zpracovatel výslovně informuje správce o všech zamýšlených změnách uvedeného seznamu přijetím nebo nahrazením dílčích zpracovatelů nejméně čtyři (4) týdny předem, čímž poskytne správci dostatek času na to, aby mohl vznést námitku proti takovým změnám před zapojením dotčeného dílčího zpracovatele / dotčených dílčích zpracovatelů. Zpracovatel poskytne správci informace nezbytné k tomu, aby správce mohl uplatnit své právo vznést námitku.

(b) Pokud zpracovatel zapojí dílčího zpracovatele do provádění konkrétních činností zpracování (jménem správce), učiní tak prostřednictvím smlouvy, která ukládá dílčímu zpracovateli v podstatě stejné povinnosti v oblasti ochrany údajů, jaké jsou v souladu s těmito Podmínkami uloženy zpracovateli osobních údajů. Zpracovatel zajistí, aby dílčí zpracovatel plnil povinnosti, které se na zpracovatele vztahují podle těchto Podmínek a nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

(c) Zpracovatel poskytne správci na jeho žádost opis dohody s dílčím zpracovatelem a veškeré následné změny dohody. V rozsahu nutném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, může zpracovatel před poskytnutím opisu text dohody upravit.

(d) Zpracovatel nese vůči správci plnou odpovědnost za to, aby dílčí zpracovatel plnil povinností vyplývající z jeho smlouvy se zpracovatelem. Zpracovatel správce uvědomí, pokud dílčí zpracovatel neplní své povinnosti vyplývající z uvedené smlouvy.

4.8. Mezinárodní předávání osobních údajů

(a) Jakékoli předání osobních údajů zpracovatelem do třetí země nebo mezinárodní organizaci se provádí pouze na základě písemně doložených pokynů správce nebo za účelem splnění konkrétního požadavku podle právních předpisů Evropské unie nebo členského státu, které se na zpracovatele vztahují, a to v souladu s kapitolou V nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.

(b) Správce souhlasí s tím, že pokud zpracovatel v souladu s článkem 4 odst. 7 těchto Pravidel zapojí dílčího zpracovatele do provádění konkrétních činností zpracováním (jménem správce) a uvedené činnosti zahrnují předání osobních údajů ve smyslu kapitoly V nařízení (EU) 2016/679, mohou zpracovatel a dílčí zpracovatel zajistit soulad s ustanoveními kapitoly V nařízení (EU) 2016/679 použitím standardních smluvních doložek přijatých Evropskou komisí v souladu s ustanovením článku 46 odst. 2 nařízení (EU) 2016/679, pokud jsou splněny standardní podmínky pro použití těchto smluvních Podmínek.

Článek 5
Pomoc poskytovaná správci

(a) Zpracovatel neprodleně informuje správce o každé žádosti, kterou obdržel od subjektu osobních údajů. Na tuto žádost neodpovídá sám, pokud k tomu není správcem zmocněn.

(b) Zpracovatel pomáhá správci při plnění jeho povinností reagovat na žádosti subjektů osobních údajů o výkon jejich práv s přihlédnutím k povaze zpracování. Při plnění svých povinností podle ustanovení písmen a) a b) postupuje zpracovatel v souladu s pokyny správce.

(c) Kromě toho, že má zpracovatel povinnost pomáhat správci podle článku 5 písm. b) těchto Podmínek, zpracovatel správci dále pomáhá při zajišťování plnění následujících povinností, a to s přihlédnutím k povaze zpracování osobních údajů a informacím, které má zpracovatel k dispozici:

(1) povinnost provést posouzení dopadu zamýšlených operací zpracování na ochranu osobních údajů (dále jen „posouzení vlivu na ochranu údajů“), pokud je pravděpodobné, že určitý druh zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob;

(2) povinnost konzultovat před zpracováním příslušný dozorový orgán, respektive příslušné dozorové orgány, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika;

(3) povinnost zajistit, aby byly osobní údaje přesné a aktuální, a to tím, že zpracovatel správce neprodleně informuje, pokud se dozví, že osobní údaje, které zpracovává, jsou nepřesné nebo zastaralé;

(4) povinnosti podle článku 32 nařízení (EU) 2016/679.

(d) V příloze II strany stanoví vhodná technická a organizační opatření, jimiž je zpracovatel povinen správci pomáhat při uplatňování této Podmínek, jakož i oblast působnosti a rozsah požadované pomoci.

Článek 6
Ohlašování případů porušení zabezpečení osobních údajů

V případě porušení zabezpečení osobních údajů zpracovatel spolupracuje se správcem a pomáhá mu při plnění jeho povinností podle článků 33 a 34 nařízení (EU) 2016/679 nebo případně podle článků 34 a 35 nařízení (EU) 2018/1725, přičemž zohlední povahu zpracování a informace, které má zpracovatel k dispozici.

6.1. Porušení zabezpečení osobních údajů zpracovávaných správcem

V případě porušení zabezpečení osobních údajů zpracovávaných správcem, zpracovatel napomáhá správci:

(a) při ohlašování případů porušení zabezpečení osobních údajů příslušnému dozorovému orgánu, respektive příslušným dozorovým orgánům, a to bez zbytečného odkladu poté, co se o něm správce dozvěděl, je-li to relevantní / (pokud je nepravděpodobné, že by porušení zabezpečení osobních údajů vedlo k ohrožení práv a svobod fyzických osob);

(b) při získávání následujících informací, které musí být podle článku 33 odst. 3 nařízení (EU) 2016/679 uvedeny v oznámení správce, a to musí přinejmenším zahrnovat:

(1) povahu daného případu porušení zabezpečení osobních údajů včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů osobních údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;

(2) pravděpodobné důsledky porušení zabezpečení osobních údajů;

(3) opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení osobních údajů, včetně případných opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

(c) při plnění povinnosti v souladu s článkem 34 nařízení (EU) 2016/679 oznámit bez zbytečného odkladu subjektu osobních údajů porušení zabezpečení osobních údajů, pokud je pravděpodobné, že dané porušení zabezpečení osobních údajů bude mít za následek vysoké riziko pro práva a svobody fyzických osob.

6.2 Porušení zabezpečení osobních údajů zpracovávaných zpracovatelem

V případě porušení zabezpečení osobních údajů zpracovávaných zpracovatelem o tom zpracovatel informuje správce bez zbytečného odkladu poté, co se o tomto porušení dozvěděl. Takové oznámení obsahuje alespoň:

(a) popis povahy daného případu porušení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů osobních údajů a záznamů osobních údajů);

(b) údaje o kontaktním místě, kde lze získat více informací o daném porušení zabezpečení osobních údajů;

(c) pravděpodobné důsledky a opatření přijatá nebo navržená k přijetí v souvislosti s porušením zabezpečení, a to včetně opatření ke zmírnění možných nepříznivých dopadů.

Pokud není možné poskytnout všechny tyto informace najednou, musí původní oznámení obsahovat informace, které jsou v dané době k dispozici, a další informace jsou poté poskytnuty bez zbytečného odkladu, jakmile jsou dostupné.

Strany stanoví v příloze II všechny další informace, které má zpracovatel poskytnout, když správci poskytuje pomoc při plnění povinností správce podle článků 33 a 34 nařízení (EU) 2016/679.

ODDÍL III – ZÁVĚREČNÁ USTANOVENÍ

Článek 7
Porušení Podmínek a ukončení smlouvy

(a) Aniž jsou dotčena jakákoli ustanovení nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725, pokud zpracovatel poruší své povinnosti podle těchto Podmínek, může mu správce nařídit, aby pozastavil zpracovávání osobních údajů, dokud zpracovatel nebude plnit povinnosti podle těchto Podmínek, nebo dokud nebude smlouva vypovězena. Zpracovatel neprodleně informuje správce v případě, že z jakéhokoli důvodu není schopen plnit ustanovení těchto Podmínek.

(b) Správce je oprávněn vypovědět smlouvu v rozsahu, v němž se týká zpracování osobních údajů v souladu s těmito Podmínkami, pokud:

(1) správce pozastavil podle písmene a) zpracovávání osobních údajů zpracovatelem a plnění povinností podle těchto Podmínek není obnoveno v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení;

(2) zpracovatel závažně nebo trvale porušuje tyto Podmínky nebo povinnosti, které pro něj vyplývají z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725;

(3) zpracovatel neplní závazné rozhodnutí příslušného soudu nebo příslušného dozorového orgánu, respektive příslušných dozorových orgánů, týkající se jeho povinností vyplývající z těchto Podmínek nebo z nařízení (EU) 2016/679 a/nebo nařízení (EU) 2018/1725.

(c) Zpracovatel je oprávněn vypovědět smlouvu v rozsahu, v němž se týká zpracování osobních údajů podle těchto Podmínek, pokud poté, co informoval správce o tom, že pokyny správce porušují platné právní požadavky podle článku 4 odst. 1 písm. b), správce na splnění těchto pokynů trvá.

(d) Po ukončení smlouvy zpracovatel podle volby správce vymaže veškeré osobní údaje zpracovávané jménem správce a potvrdí správci, že tak učinil, nebo vrátí veškeré osobní údaje správci a vymaže stávající kopie, pokud právo Evropské unie nebo členského státu nepožaduje uchovávání osobních údajů. Dokud nejsou osobní údaje vymazány nebo vráceny, zpracovatel nadále zajišťuje dodržování souladu s těmito Podmínkami.

PŘÍLOHA I

POPIS ZPRACOVÁNÍ

Zpracovatelská činnost: Servis, Podpora, Poradenství, Administrace, Vzdálená údržba

- Kdy nastává zahájení zpracování osobních údajů: zahájením servisní smlouvy
- Jaká je plánovaná doba trvání zpracování osobních údajů: do ukončení servisní smlouvy

Základní podmínky zpracování osobních údajů a povinnosti stran týkající se obchodního smluvního vztahu jsou specifikovány v smlouvě o poskytování služeb uzavřené mezi správcem a zpracovatelem.

Kategorie subjektů osobních údajů, povaha/účel zpracování osobních údajů, kategorie osobních údajů a jakékoli zvláštní kategorie osobních údajů závisí na typu poskytované služby, a na osobních údajích uložených zákazníkem, ke kterým má společnost Olympus přístup v průběhu poskytování služby.

Kategorie subjektů osobních údajů	**Oblasti zpracovávání**	**Kategorie osobních údajů**	**Zvláštní kategorie osobních údajů – pokud je relevantní**
☒ Pacienti ☒ Kontaktní osoby ☒ Zaměstnanci ☒ Bývalí zaměstnanci ☒ Dodavatelé a jejich zaměstnanci	☒ Provoz a údržba IT systémů a infrastruktury, např. analytických systémů ☒ konzultace ohledně používání produktů ☒ IT podpora ☒ Technická podpora ☒ Administrace ☒ Opravy, testování nebo údržba na místě nebo v opravárenském centru společnosti Olympus ☒ Vzdálená diagnostika hardwarových produktů ☒ Vzdálené testování / údržba softwarových produktů ☒ Zapůjčení zdravotnického prostředku	☒ Informace o účtu ☒ Společnost ☒ Datum narození ☒ Souhlasy a oprávnění pro zdravotnický prostředek ☒ ID a/nebo název zdravotnického prostředku ☒ Přihlašovací údaje k zdravotnickému prostředku ☒ E-mailová adresa ☒ Pohlaví ☒ Identifikátor (analytický, smlouva, zdravotnický prostředek) ☒ Jazyk ☒ Poloha ☒ Protokoly (Logy); ☒ Jméno ☒ Uživatelské jméno	☒ Zdravotní údaje (například informace o zdravotním stavu pacienta)

		☒ Základní údaje uživatele ☒ Údaje o používání (IP adresa, záznamy o přihlášení, telefonní záznamy) ☒ Údaje o používání zdravotnického prostředku a systémů ☒ Obrazové a video data	

Práce se zdravotnickým prostředkem může vyžadovat kopírování a analýzu souboru protokolu (log file). Soubor protokolu může obsahovat jména pacientů. Podpora první a druhé úrovně je poskytována v rámci EU. Podpora třetí úrovně je poskytována subjektem Olympus se sídlem v USA („Olympus Surgical Technologies America“). Proto, je-li pro řešení problému vyžadována podpora třetí úrovně, může být nezbytné předat osobní data do Spojených států. Za účelem zajištění odpovídající úrovně ochrany uzavřel Olympus příslušné interní dohody o zpracování osobních údajů (DPA) se svými přidruženými subjekty v USA.

PŘÍLOHA II

TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ, VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K ZAJIŠTĚNÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

S ohledem na stav techniky, náklady na provedení, povahu, rozsah, kontext a účely zpracování, jakož i s ohledem na různou pravděpodobnost a závažnost rizika pro práva a svobody fyzických osob, přijme Zpracovatel následující technická a organizační opatření:

OPATŘENÍ	POPIS
1. DŮVĚRNOST	
a) Kontrola přístupu – prostory společnosti Olympus	Budovy společnosti Olympus jsou nepřetržitě uzavřené a střežené. Zaměstnanci mohou vstupovat do budov pouze pomocí své osobní identifikační karty. Návštěvníci mohou vstoupit do budov pouze přes recepci a v doprovodu zaměstnance. Nepovoleným osobám je vstup do budov zakázán. Následující bezpečnostní opatření jsou implementována: - Identifikační karty zaměstnanců / návštěvníků - Systém kontroly vstupu, čtečka karet, transpondér, magnetické a čipové karty - Lobby / recepční / vrátný - (Kontrolované) klíče / přidělování klíčů - Zámky dveří (elektrické otevírání dveří, dveře s vnějším klikem, apod.) - Průmyslová bezpečnost, vrátný - Systém sledování, poplachový systém, video-monitorování / TV monitorování
b) Kontrola přístupu – systémy	Všechny systémy jsou instalovány v zabezpečených datových centrech a chráněny osobními identifikačními kartami v kombinaci s PIN kódem. Následující bezpečnostní opatření jsou implementována: - Zabezpečení pomocí hesel (včetně speciálních znaků, minimální délky, pravidelná změna hesel); - Automatické zamykací mechanismy (např. zamykání po zadání hesla nebo pauze, automatické zamykání pracovní plochy); - Pokyny pro manuální zamykání pracovní plochy; - Nastavení a správa uživatelského profilu a kmenového záznamu; - Firewall, antivirový software pro servery a klienty; - Použití VPN pro vzdálený přístup; - Politika pro mobilní zařízení (Mobile Device Policy).

c) Kontrola přístupu – správa práv: oprávnění ke čtení a úpravám interních IT systémů Olympus	Pro používání IT systémů je zaveden systematický management práv. Přístup k systémům je možný pouze pomocí uživatelského jména a hesla. Oprávnění se liší mezi právy ke čtení a právem k úpravám. Následující bezpečnostní opatření jsou implementována: - Diferencovaný koncept oprávnění a přístupová práva založená na principu „need to know“ (profily, role, transakce a objekty)
d) Kontrola oddělení interních IT systémů Olympus	Vzdálená údržba je prováděna samostatně pro každého zákazníka. Následující bezpečnostní opatření jsou implementována: - Víceuživatelská schopnost příslušných aplikací - Označování (Earmarking); - Oddělení funkcí produktivního a testovacího prostředí; - Fyzické oddělení systémů, databází a nosičů dat; - Definice práv k databázím.
e) Šifrování	Je upřednostněna šifrovaná komunikace. Použitá šifrovací metoda odpovídá stavu techniky.
2. INTEGRITA	
a) Kontrola transfer interních IT systémů Olympus	Následující bezpečnostní opatření jsou implementována: - V rámci sítě je možné šifrovat e-maily; - V systému není povoleno neoprávněné čtení, kopírování, upravování ani odstraňování dat; - Použití VPN, stejně jako poskytování přístupu prostřednictvím šifrovaných spojení, například sftp nebo https.
b) Vstupní kontrola	Změny v systémech jsou zaznamenávány. Následující bezpečnostní opatření jsou implementována: - Zaznamenávání přístupů (logging); - Systémy pro vyhodnocování logů a sledovatelnost zadávání, úprav a mazání dat podle jednotlivých uživatelských jmen; - Přidělování práv prostřednictvím personalizovaných uživatelských účtů; - Správa dokumentů (Document management).
3. DOSTUPNOST A ODOLNOST	

a) Kontrola dostupnosti; opatření na ochranu dat v interních systémech Olympus	Osobní údaje jsou zabezpečeny. Je zajištěna ochrana proti náhodnému nebo úmyslnému zničení či ztrátě, stejně jako kontrola dostupnosti dat. Následující bezpečnostní opatření jsou implementována: - Postup při zálohování: popis frekvence a média zálohy, doba a místo uchovávání zálohy (online/offline, na místě/mimo místo); - Zrcadlení pevných disků, např. postup RAID; - Nepřerušitelný zdroj napájení (UPS); - Oddělené úložiště nebo oddíl pro operační systémy a data; - Ochrana proti virům a firewall; - Kanály pro hlášení a havarijní plány; - Hasicí přístroje a poplachové systémy v budovách, zejména v serverovně, kde je také monitorována teplota a vlhkost, a jsou instalovány ochranné zásuvkové lišty.
b) Rychlé obnovení	Za obnovení dat nese odpovědnost správce.
4. POSTUPY PRO PRAVIDELNÉ PŘEZKOUMÁVÁNÍ, HODNOCENÍ A POSUZOVÁNÍ	
a) Kontrola zakázek u interních IT systémů Olympus	Účinnost přijatých opatření je pravidelně přezkoumávána. Kontrola zakázek je prováděna náhodně. Následující bezpečnostní opatření jsou implementována: - Jasná textace smlouvy; - Formalizované zadávání zakázek; - Výběr dodavatele s ohledem na náležitou péči (zejména z hlediska ochrany osobních údajů a bezpečnosti); - Uzavření potřebné smlouvy o zpracování zakázka nebo použití standardních smluvních doložek (podmínek) EU; - Zadávání pokynů dodavateli písemně nebo v textové formě; - Povinnost zaměstnanců dodavatele zachovávat mlčenlivost o osobních údajích; - Povinnost dodavatele jmenovat pověřence pro ochranu osobních údajů, pokud taková povinnost existuje podle objednávky; - Dohoda o účinných kontrolních právech vůči dodavateli; - Ujednání o použití dalších subdodavatelů; - Zajištění zničení dat po dokončení zakázky; - Průběžná kontrola dodavatele a jeho úrovně ochrany.

b) Řízení ochrany osobních údajů a reakce na incidenty	- Centrální dokumentace všech postupů a předpisů týkajících se ochrany údajů s přístupem pro zaměstnance podle potřeby / oprávnění; - Interní pracovník pro informační bezpečnost a ochranu osobních údajů; - Pravidelná školení zaměstnanců a závazek k mlčenlivosti / ochraně soukromí; - Dokumentovaný proces pro rozpoznávání a hlášení bezpečnostních incidentů / porušení dat (včetně povinného hlášení příslušným dozorovým orgánům); - Dokumentovaný postup pro řešení bezpečnostních incidentů a porušení ochrany dat; - Formalizované posouzení dopadů na ochranu soukromí (Privacy Impact Assessment) a proces pro vyřizování žádostí o informace od subjektů osobních údajů.

PŘÍLOHA III

SEZNAM DÍLČÍCH ZPRACOVATELŮ

Správce povolil a souhlasí s využitím následujících dílčích zpracovatelů:

Obchodní firma a adresa	**Jméno kontaktní osoby, její pozice a kontaktní údaje**	**Popis zpracování**	**Pokud je to relevantní, záruky pro předávání do třetích zemí**
Olympus Europa SE & Co. KG Wendenstraße 20 20097 Hamburg Germany	Stefan Limbacher Pověřenec pro ochranu osobních údajů region EMEA privacy@olympus.com	Druhá úroveň podpory pro opravy, údržbu a vzdálenou údržbu softwaru a zdravotnických prostředků.	ano/ne, dílčí zpracovatel usazený v Hamburku, Německu
Olympus Surgical Technologies Europe **Olympus Winter & Ibe GmbH** Kuehnstraße 61 22045 Hamburg Germany	privacy@olympus.com	Třetí úroveň podpory pro opravy, údržbu a vzdálenou údržbu softwaru a zdravotnických prostředků.	Ano/ne, dílčí zpracovatel usazený v Hamburku, Německu
Olympus Medical Systems Corporation 2951 Ishikawa-machi, Hachioji-shi Tokyo 192-8507 Japan	privacy@olympus.com	Řešení stížností, včetně šetření závad a neočekávaných chyb.	Rozhodnutí o vhodné úrovni ochrany (EU) 2019/419 Evropské komise

Olympus Surgical Technologies America 800 W Park Dr. Westborough, MA 01581 USA	privacy@olympus.com	Řešení stížností, včetně šetření závad a neočekávaných chyb.	Standardní smluvní doložky (podmínky)
Tata Consultancy Services GmbH Friedrich-Ebert-Anlage 49 60308 Frankfurt am Main Germany	privacy@olympus.com	Poskytovatel IT infrastruktury a služeb	Ano/ne, dílčí zpracovatel usazený ve Frankfurtu, Německu
TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen Germany	privacy@teamviewer.com	Dozor a kontrola počítačových systémů	Ano/ne, dílčí zpracovatel usazený v Göppingen, Německu
ImageStreamMedical One Monarch Drive Littleton, MA 01460 USA	privacy@cision.com	Třetí úroveň podpory pro opravy, údržbu a vzdálenou údržbu softwaru.	Standardní smluvní doložky (podmínky)
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521 Ireland	privacy@microsoft.com	Různé cloudové služby	Ano/ne, dílčí zpracovatel usazený v Irsku

RealVNC Limited 50-60 Station Road Cambridge Cambridgeshire CB1 2JH United Kingdom of Great Britain and Northern Ireland	privacy@realvnc.com	Poskytovatel softwaru pro vzdálené ovládání pro SPiN Planning Laptop Workstation – bez ukládání dat, pouze šifrované sdílení obrazovky	Rozhodnutí o vhodné úrovni ochrany pro Spojené království