

VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE
Správa účelových zařízení

PŘÍKAZ ŘEDITELE SÚZ VŠE

č. 8/2022

Ev. č.: VŠE/2568/2022

Čj.: VŠE/1975/7000/2022

V Praze dne 25. 3. 2022

ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ

na Správě účelových zařízení VŠE

S účinností od 01. 04. 2022 vydávám tento příkaz, který je určen pro vnitřní potřebu Správy účelových zařízení VŠE. Gestorem těchto Zásad je Ing. Jan Zavřel.

Tímto příkazem ruším příkaz č. 5/2018.

Ing. Ota Zima CSc., MBA v.r.
ředitel SÚZ VŠE

OBSAH

1.	Preambule	3
2.	Definice a pojmy.....	3
3.	Garant zpracování osobních údajů, pověřenec pro ochranu osobních údajů VŠE	4
4.	Kategorie subjektů údajů	4
5.	Způsob evidence a uchování osobních údajů.....	6
6.	Definice práv, povinností a odpovědnosti za evidenci a zpracování osobních údajů.....	8
7.	Způsoby zabezpečení osobních údajů a eliminace rizik bezpečnostních incidentů	13
7.1.	Principy zabezpečení tištěných dokumentů	13
7.2.	Principy zabezpečení elektronických souborů	14
7.2.1.	osobní údaje:	14
7.2.2.	kamery záznamy:	14
7.3.	Principy použití a zabezpečení počítačů Organizace a služebních mobilních telefonů	14
7.4.	Principy tvorby a správy přístupových hesel	14
7.5.	Principy ochrany a hierarchizace přístupů do informačních systémů	14
7.6.	Principy zabezpečení informačních systémů.....	14
7.7.	Principy využití elektronické pošty pro přenos osobních údajů	15
7.8.	Předávání tištěných dokumentů obsahujících osobní údaje uvnitř Organizace.....	15
8.	Systém testování přijatých opatření na eliminaci rizik	15
9.	Principy kopírování dokumentů s osobními údaji	15
10.	Způsoby zabezpečení provozoven.....	15
11.	Principy zálohování, archivace a obnovy osobních údajů	16
12.	Zásady skartace tištěných i elektronických médií s osobními údaji	16
13.	Vyřizování požadavků subjektů údajů	16
14.	Proces vedení záznamů o činnosti zpracování osobních údajů.....	16
15.	Principy profilování.....	16
16.	Zásady předávání osobních údajů do zahraničí.....	16
17.	Systém odhalování bezpečnostních incidentů	16
18.	Systém informování Úřadu a subjektů údajů o bezpečnostních incidentech	16
19.	Principy motivačního systému k dodržování zásad bezpečnosti osobních údajů	17
20.	Definice odpovědnosti zaměstnanců za bezpečnost osobních údajů	17
21.	Pravidla pro používání soukromých elektronických zařízení	17
22.	Principy práce z domova	17
23.	Pravidla používání elektronických zařízení a médií s osobními údaji mimo prostory provozovny.....	17
24.	Zásady školení zaměstnanců v oblasti bezpečnosti osobních údajů	17
25.	PŘÍLOHY.....	18

1. Preambule

Ochrana osobních údajů fyzických osob je základním právem daným Listinou základních práv Evropské unie. Fyzické osoby mají zaručenou právní i praktickou jistotu ochrany svých osobních údajů a musí mít možnost kontrolovat své vlastní osobní údaje.

Tento příkaz ředitele stanoví pravidla a postupy v oblasti ochrany osobních údajů a bezpečnosti jejich zpracování. Při zpracování osobních údajů musí být dodržováno 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 (dále Nařízení) a s ním související legislativa České republiky zejména zákon č. 110/2019 Sb. o zpracování osobních údajů a zákon č. 111/2019 Sb. kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Tento příkaz ředitele se vydává v souladu se směrnicí Vysoké školy ekonomické v Praze SR 05/2018 v platné verzi, „Ochrana a zpracování osobních údajů“ a upravuje specifické oblasti zpracování osobních údajů na Správě účelových zařízení Vysoké školy ekonomické v Praze.

Tento vnitřní předpis je závazný pro všechny zaměstnance Organizace.

2. Definice a pojmy

Definice pojmů vychází z Článku 4 Nařízení. Zde pro přehlednost uvádíme nejdůležitější definice:

Osobní údaje	veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“).
Subjekt údajů	identifikovatelná fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
Kategorie subjektů údajů	např. zaměstnanci, uchazeči o zaměstnání, zákazníci (fyzické osoby), dodavatelé (fyzické osoby), osoby pohybující se v areálu Organizace atd.
Souhlas	jakýkoli svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů.
Pseudonymizace osobních údajů	zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.
Zpracování osobních údajů	jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
Zvláštní kategorie osobních údajů (citlivé osobní údaje)	rasový či etnický původ, zdravotní stav, genetické údaje, biometrické údaje, politické názory, náboženské vyznání nebo přesvědčení, filozofické přesvědčení, členství v odborech, sexuální orientace, sexuální život.

Organizace	Správa účelových zařízení Vysoké školy ekonomické v Praze, se sídlem Jeseniova 2769/208, 130 00 Praha 3, IČ VŠE: 61384399.
Garant zpracování osobních údajů	Osoba odpovědná za dodržování zásad, pravidel a postupů (uvedených v SR 05/2018 a tímto příkazu ředitele jakož i v Nařízení a dalších obecně závazných právních předpisech) při zpracování osobních údajů v Organizaci včetně zajištění vypořádání práv subjektů údajů.
Úřad	Úřad pro ochranu osobních údajů (ÚOOÚ).
Zaměstnanec	fyzická osoba, která je s Organizací v pracovněprávním vztahu (pracovním poměru nebo ve vztahu založeném dohodou o pracích konaných mimo pracovní poměr).

3. Garant zpracování osobních údajů, pověřenec pro ochranu osobních údajů VŠE

Garantem zpracování osobních údajů v Organizaci je ustanoven Ing. Jan Zavřel, e-mail: gdpr-suz@vse.cz, telefon: 22409 2118.

Pověřencem pro ochranu osobních údajů Vysoké školy ekonomické v Praze (DPO VŠE) je RNDr. Karel Nenadál, e-mail: dpo@vse.cz, telefon: 22409 5710.

Garant zpracování osobních údajů zodpovídá za implementaci tohoto vnitřního předpisu v Organizaci. Organizuje pravidelné školení zaměstnanců Organizace podle kapitoly 24. tohoto příkazu ředitele. Sleduje vývoj v oblasti ochrany osobních údajů jak z hlediska legislativních změn, tak z hlediska změn v technologii zpracování osobních údajů a zajišťuje implementaci nastalé změny do praxe Organizace. Organizuje uzavření smluv se zpracovatelem osobních údajů a s dodavatelem služeb, jejichž pracovníci se pohybují v prostorách Organizace. Jedná se zejména o dodavatele informačních systémů ISKAM, KREDIT a BOOKOLO, o školitele PO, BOZP a řidičů a o pracovníky úklidové služby. Dále za uzavření doložky k servisní smlouvě s provozovatelem kamerového systému ALSIG.

Je odpovědný za včasné vyřizování požadavků subjektů údajů podle kapitoly 13. tohoto příkazu ředitele.

Ve spolupráci s DPO VŠE je odpovědný za včasné informování Úřadu a popř. i subjektů údajů o bezpečnostních incidentech podle kapitoly 18. tohoto příkazu ředitele.

Pravidelně čtvrtletně (v případě nutnosti neprodleně) informuje ředitele Organizace o stavu zabezpečení osobních údajů na všech úrovních Organizace a projednává s ním návrhy opatření na zdokonalení systému zabezpečení osobních údajů.

Neprodleně informuje ředitele Organizace a DPO VŠE o nastalých bezpečnostních incidentech, o jejich dopadu na Organizaci a na případné porušení práv a svobod subjektů údajů. Zároveň jim předkládá návrhy na eliminaci příčin těchto bezpečnostních incidentů.

4. Kategorie subjektů údajů

Organizace pro níže definované kategorie subjektů údajů zpracovává osobní údaje v rozsahu:

Kategorie subjektů údajů	Maximální rozsah evidovaných a zpracovávaných osobních údajů
Studenti VŠE	jméno, příjmení, rodné číslo, datum narození, číslo bankovního účtu, trvalé bydliště, kamerový záznam, fotografie, identifikační číslo studenta, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, e-mail VŠE, číslo OP, číslo platební karty, státní příslušnost, pohlaví;
Studenti jiných VŠ	jméno, příjmení, rodné číslo, datum narození, číslo bankovního účtu, trvalé bydliště, kamerový záznam, fotografie, identifikační číslo studenta, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, e-mail vysoké školy, číslo OP, číslo platební karty, státní příslušnost, pohlaví;

Kategorie subjektů údajů	Maximální rozsah evidovaných a zpracovávaných osobních údajů
Zahraniční studenti	jméno, příjmení, datum narození, číslo bankovního účtu, trvalé bydliště, kamerový záznam, fotografie, identifikační číslo studenta, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, e-mail VŠE, číslo OP, číslo pasu, adresa pobytu v ČR, číslo platební karty, podpis, státní příslušnost, pohlaví;
Hoteloví hosté	jméno, příjmení, datum narození, trvalé bydliště, kamerový záznam, číslo platební karty, podpis, státní příslušnost;
Hoteloví hosté – cizinci	jméno, příjmení, datum narození, místo narození, trvalé bydliště, kamerový záznam, číslo pasu, adresa pobytu v ČR, číslo platební karty, podpis, státní příslušnost;
Potenciální hoteloví hosté	jméno, příjmení, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, státní příslušnost;
Nájemníci bytů	jméno, příjmení, datum narození, trvalé bydliště, kamerový záznam, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, e-mail v Organizaci/zaměstnání
Zaměstnanci Organizace	jméno, příjmení/rodné příjmení, rodné číslo, datum narození, místo narození, číslo bankovního účtu, trvalé bydliště, korespondenční adresa, kamerový záznam, fotografie, identifikační číslo zaměstnance, zdravotní pojišťovna, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, telefonní číslo Organizace, číslo mobilního telefonu Organizace, e-mail v Organizaci, evidence jízd, číslo OP, číslo pasu, adresa pobytu v ČR, podpis, státní příslušnost, pohlaví, zdravotní postižení;
Uchazeči o zaměstnání	jméno, příjmení, datum narození, trvalé bydliště, korespondenční adresa, kamerový záznam, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail;
Dodavatelé	jméno, příjmení, číslo bankovního účtu, kamerový záznam, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, firemní telefonní číslo, číslo firemního mobilního telefonu, firemní e-mail, IČ, adresa sídla podnikání, místo podnikání, DIČ,
Odběratelé	jméno, příjmení, číslo bankovního účtu, kamerový záznam, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, firemní telefonní číslo, číslo firemního mobilního telefonu, firemní e-mail, IČ, adresa sídla podnikání, místo podnikání, DIČ;
Uživatelé parkoviště	jméno, příjmení, kamerový záznam, SPZ vozidla, soukromé telefonní číslo, číslo soukromého mobilního telefonu, soukromý e-mail, barva a typ vozidla;
Osoby podávající stížnost	jméno, příjmení, soukromý e-mail, e-mail VŠE;
Děti zaměstnance	jméno, příjmení, rodné číslo, datum narození, místo narození, trvalé bydliště, pohlaví, zdravotní postižení;
Manžel/manželka zaměstnance	jméno, příjmení, rodné číslo, datum narození, trvalé bydliště;
Strávníci menzy	jméno, příjmení, datum narození, kamerový záznam;
Osoby procházející areálem Kampusu Jarov	Kamerový záznam;
Osoby s rezervací sportoviště	jméno, příjmení, kamerový záznam, číslo soukromého telefonu/mobilního telefonu, soukromý e-mail;
Návštěvy	jméno, příjmení, kamerový záznam, číslo OP/číslo pasu.

5. Způsob evidence a uchování osobních údajů

Osobní údaje jsou evidovány a uchovávány v těchto formách:

Dokument, agenda	Forma	Kategorie subjektů údajů
Informace o studujících	informační systém InSIS	Studenti VŠE, Zahraniční studenti;
Informace o ubytovaných	informační systém ISKAM, InSIS a přístupový systém SÚZ	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti, Hoteloví hosté, Hoteloví hosté – cizinci, Potenciální hoteloví hosté;
Informace o stravovaných v menzách	informační systém KREDIT	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti, Zaměstnanci, Strávníci menzy;
Mzdová a personální agenda	informační systém EGJE	Zaměstnanci, Děti zaměstnanců, Manželky/manželé zaměstnanců;
Účetní agenda	informační systém IFIS	Nájemníci bytů, Dodavatelé, Odběratelé;
Přehled korespondence	informační systém ATENA	Zaměstnanci, Uchazeči o zaměstnání, Dodavatelé, Odběratelé;
Ubytování v hotelech	informační systém BOOKOLO	Hoteloví hosté, Hoteloví hosté-cizinci, potencionální hoteloví hosté;
Kamerový záznam	elektronický soubor	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti, Hoteloví hosté, Hoteloví hosté – cizinci, Nájemníci bytů, Zaměstnanci, Uchazeči o zaměstnání, Dodavatelé, Odběratelé, Uživatelé parkoviště, Strávníci menzy, Osoby s rezervací sportoviště, Osoby procházející kampusem Jarov, Návštěvy;
Přístupový systém SÚZ	přístupový systém MC SYSTEMS	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti;
Rezervace sportovišť	informační systém eSports	Osoby s rezervací sportoviště;
Telefonní seznam	elektronický soubor	Zaměstnanci;
Životopisy uchazečů o zaměstnání	tištěný dokument, e-mail	Uchazeči o zaměstnání;
Životopisy zaměstnanců	tištěný dokument, e-mail	Zaměstnanci;
Doklady o vzdělání	tištěný dokument, e-mail	Zaměstnanci, Uchazeči o zaměstnání;
Osobní dotazník, přehled praxe	tištěný dokument	Zaměstnanci;
Lékařské prohlídky	tištěný dokument	Zaměstnanci;
Informace pro nastupující zaměstnance	tištěný dokument	Zaměstnanci;
Pracovní smlouvy	tištěný dokument, informační systém EGJE	Zaměstnanci;
Mzdový výměr	tištěný dokument	Zaměstnanci;
Změnové hlášení	tištěný dokument, e-mail	Zaměstnanci;
Evidenční list důchodového pojištění	tištěný dokument, informační systém EGJE	Zaměstnanci;
Exekuce	tištěný dokument	Zaměstnanci;
Mzdové sestavy	tištěný dokument, informační systém EGJE	Zaměstnanci;
Penzijní pojištění	tištěný dokument	Zaměstnanci;
Potvrzení o seznámení s vnitřním předpisem ochrany osobních údajů	tištěný dokument, elektronický soubor	Zaměstnanci;
Faktury přijaté	tištěný dokument, e-mail	Dodavatelé;

Dokument, agenda	Forma	Kategorie subjektů údajů
Faktury vydané	tištěný dokument, e-mail	Odběratelé;
Evidence majetku	tištěný dokument informační systém IFIS	Zaměstnanci;
Knihy jízd	tištěný dokument	Zaměstnanci;
Cestovní příkazy	tištěný dokument, informační systém EGJE	Zaměstnanci;
Evidence pošty	tištěný dokument, informační systém ATENA	Zaměstnanci, Uchazeči o zaměstnání, Dodavatelé, Odběratelé;
Záznam poučení při poskytnutí údajů	tištěný dokument	Zaměstnanci;
Seznam uživatelů parkoviště	elektronický soubor	Uživatelé parkoviště;
Evidence parkovacích lístků	elektronický soubor	Uživatelé parkoviště;
Evidence dodavatelů	tištěný dokument, e-mail, elektronický soubor, služební mobilní telefon	Dodavatelé;
Evidence odběratelů	tištěný dokument, e-mail, elektronický soubor, služební mobilní telefon	Odběratelé;
Smlouvy (mimo pracovních)	tištěný dokument, elektronický soubor, informační systém	Dodavatelé, Odběratelé, Nájemníci bytů;
Stížnosti / odpovědi na stížnosti	tištěný dokument, e-mail, elektronický soubor	Osoby podávající stížnost;
Smlouvy o ubytování + dodatky	tištěný dokument	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti;
Doklad pro cizineckou policii	tištěný dokument	Zahraniční studenti, Hoteloví hosté-cizinci;
Formulář při odchodu	tištěný dokument	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti, Zaměstnanci;
Kolejní průkaz	tištěný dokument	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti,
Doklad o zaplacení kolejného	tištěný dokument	Studenti VŠE, Studenti jiných VŠ, Zahraniční studenti;
Kontakty na hotelové zaměstnance	tištěný dokument, elektronický soubor, služební mobilní telefon	Zaměstnanci;
Domovní kniha	tištěný dokument	Hoteloví hosté – cizinci;
Přihlašovací lístek	tištěný dokument	Hoteloví hosté, Hoteloví hosté – cizinci;
Rodné listy dětí zaměstnanců – kopie	tištěný dokument	Děti zaměstnanců;
Čestné prohlášení	tištěný dokument	Zaměstnanci;
Záznam o školení řidičů	tištěný dokument	Zaměstnanci;
Záznam o školení PO a BOZP	elektronický soubor	Zaměstnanci;
Evidence odpracovaných hodin pracovníků údržby	elektronický soubor, tištěný dokument	Zaměstnanci;
Seznam klíčů	elektronický soubor	Zaměstnanci;
Žádanky na objednávku	tištěný dokument	Zaměstnanci, Dodavatelé;

Dokument, agenda	Forma	Kategorie subjektů údajů
Potvrzení o seznámení s vnitřním předpisem ochrany osobních údajů	tištěný dokument	Zaměstnanci;
Evidenze návštěv	informační systém	Návštěvy.

6. Definice práv, povinností a odpovědnosti za evidenci a zpracování osobních údajů

Odpovědné osoby uvedené v této kapitole jakož i jim podřízené osoby jsou povinny zpracovávat osobní údaje vždy jen v rozsahu podmínek realizace řešení příslušného zpracování osobních údajů. Dále jsou povinny zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i po ukončení pracovního poměru.

Pokud podle článku 6, odst. 1. Nařízení je pro zákonnost zpracování osobních údajů v daném rozsahu splněno více podmínek, nebude zpracování osobních údajů prováděno na základě podmínky dle písmeno a). „Zpracovávání na základě souhlasu“.

6.1. Řízení lidských zdrojů

Odpovědná osoba: Vedoucí oddělení řízení lidských zdrojů.

Eviduje a zpracovává: osobní údaje zaměstnanců v informačním systému EGJE, v e-mailové poště a osobní údaje zaměstnanců a uchazečů o zaměstnání v tištěných dokumentech:

životopisy uchazečů o zaměstnání,
životopisy zaměstnanců,
doklady o vzdělání,
osobní dotazníky, přehled praxe,
potvrzení o seznámení s vnitřním předpisem „zásady ochrany osobních údajů“,
doklady o lékařských prohlídkách,
informace pro nastupující zaměstnance,
pracovní smlouvy,
mzdové výměry,
změnová hlášení,
evidenční listy důchodového pojištění,
exekuce,
mzdové sestavy,
penzijní pojištění,
formulář při odchodu zaměstnance,
kopie rodných listů dětí,
čestná prohlášení.

Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v informačním systému EGJE, v e-mailové poště a v tištěných dokumentech.

Dodržení předepsaného rozsahu osobních údajů evidovaných v informačním systému EGJE a v jím spravovaných dokumentech a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.

Za získání souhlasů s případnou evidencí osobních údajů uchazečů o zaměstnání.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává, a to včetně dokumentů umístěných v archivu Organizace.

Smazání všech záznamů v informačních systémech, e-mailech a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.2. Sekretariát ředitele

Odpovědná osoba: Pracovnice sekretariátu.

Eviduje a zpracovává: Osobní údaje zaměstnanců, uchazečů o zaměstnání, dodavatelů a odběratelů evidované v informačním systému ATENA a osobní údaje zaměstnanců, uchazečů o zaměstnání, dodavatelů a odběratelů v tištěných dokumentech:
knihy jízd,
cestovní příkazy,
evidence pošty,
záznam poučení při poskytnutí údajů,
záznam o školení řidičů,
kopie smluv s dodavateli,
nájemní smlouvy.
Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v informačním systému ATENA a v tištěných dokumentech.
Dodržení předepsaného rozsahu osobních údajů evidovaných v informačním systému ATENA a v jím spravovaných dokumentech a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.
Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.
Smazání všech záznamů v informačních systémech a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.
Za včasnou identifikaci případného bezpečnostního incidentu.
Za identifikaci potencionálních hrozeb narušení bezpečnosti osobních údajů.

6.3. Právní útvar

Odpovědná osoba: Vedoucí Právního oddělení.

Eviduje a zpracovává: Osobní údaje zaměstnanců, dodavatelů, odběratelů a osob podávajících stížnost v tištěných dokumentech, elektronických souborech, e-mailech a registru smluv VŠE:
smlouvy s dodavateli,
smlouvy s odběrateli,
evidence odběratelů,
stížnosti,
odpovědi na stížnosti.
Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v tištěných dokumentech, elektronických souborech, e-mailech a registru smluv VŠE.
Dodržení předepsaného rozsahu osobních údajů v jím spravovaných dokumentech a agendách a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.
Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.
Smazání všech záznamů v elektronických souborech, registru smluv VŠE a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.
Za včasnou identifikaci případného bezpečnostního incidentu.
Za identifikaci potencionálních hrozeb narušení bezpečnosti osobních údajů.

6.4. Investiční a stavební oddělení

Odpovědná osoba: Vedoucí Investičního a stavebního oddělení.

Eviduje a zpracovává: Osobní údaje dodavatelů v tištěných dokumentech, elektronických souborech, e-mailech a služebním mobilním telefonem. Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v tištěných dokumentech, elektronických souborech, e-mailech a služebním mobilním telefonu. Dodržení předepsaného rozsahu osobních údajů v jím spravovaných dokumentech a agendách a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2. Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává. Smazání všech záznamů v elektronických souborech, e-mailech a služebních mobilních telefonech a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci. Za včasnou identifikaci případného bezpečnostního incidentu. Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.5. Vedení účetnictví

Odpovědná osoba: Vedoucí ekonomického oddělení.

Eviduje a zpracovává: Osobní údaje dodavatelů a odběratelů, osob ubytovaných ve služebních bytech, osob, které mají pronajaté nebytové prostory v informačním systému IFIS a v tištěných dokumentech:
faktury přijaté,
faktury vydané.
Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v informačním systému IFIS a v tištěných dokumentech. Dodržení předepsaného rozsahu osobních údajů evidovaných v informačním systému IFIS a v jím spravovaných tištěných dokumentech a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2. Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává. Smazání všech záznamů v informačních systémech a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci. Za včasnou identifikaci případného bezpečnostního incidentu. Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.6. Evidence majetku

Odpovědná osoba: Vedoucí ekonomického oddělení.

Eviduje a zpracovává: Osobní údaje zaměstnanců v tištěném dokumentu evidence majetku a v systému IFIS. Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v tištěném dokumentu evidence majetku. Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává. Smazání všech záznamů a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci. Za včasnou identifikaci případného bezpečnostního incidentu. Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.7. Správa ubytovacího systému

Odpovědná osoba: Správce databáze ISKAM.

Zpracovává: Osobní údaje studentů VŠE, studentů jiných VŠ, zahraničních studentů, hotelových hostů, hotelových hostů-cizinců, potenciálních hotelových hostů a ostatních ubytovaných osob v informačním systému ISKAM a InSIS.

Odpovídá za: Zajištění provozu informačního systému ISKAM.
Za včasnou identifikaci případného bezpečnostního incidentu.
Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.8. Nákup a správa IT

Odpovědná osoba: Vedoucí ekonomického oddělení.

Eviduje a zpracovává: Osobní údaje dodavatelů v elektronickém souboru a v služebním mobilním telefonu. Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v elektronickém souboru a v služebním mobilním telefonu.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Smazání všech záznamů v elektronických souborech a služebním mobilním telefonu obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a zpracování.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.9. Správa parkoviště

Odpovědná osoba: Vedoucí ekonomického oddělení.

Eviduje a zpracovává: Osobní údaje uživatelů parkoviště v elektronických souborech Seznam uživatelů parkoviště a Evidence parkovacích lístků. Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v elektronických souborech Seznam uživatelů parkoviště a Evidence parkovacích lístků.

Dodržení předepsaného rozsahu osobních údajů evidovaných v elektronických souborech a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Smazání všech záznamů v elektronických souborech obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.10. Obchodní oddělení

Odpovědná osoba: Vedoucí Obchodního oddělení.

Eviduje a zpracovává: Osobní údaje studentů VŠE, studentů jiných VŠ, zahraničních studentů, hotelových hostů, hotelových hostů-cizinci, potenciálních hotelových hostů v informačním systému ISKAM a BOOKOLO. Kamerové záznamy osob pohybujících se v areálu spravovaném Organizací. Zpracovává údaje o studentech VŠE v informačním systému InSIS. Podrobnosti viz příloha č. 2.

Odpovídá za: Bezpečnost, úplnost aktuálnost a integritu osobních údajů evidovaných v informačním systému ISKAM a BOOKOLO.

Dodržení předepsaného rozsahu osobních údajů evidovaných v informačních systémech ISKAM a BOOKOLO a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Smazání všech záznamů v informačních systémech ISKAM a BOOKOLO obsahujících osobní údaje subjektů údajů a skartování všech tištěných dokumentů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.11. Provozní oddělení

Odpovědná osoba: Vedoucí Provozního oddělení.

Eviduje a zpracovává: Zpracovává osobní údaje v tištěných a elektronických dokumentech v rámci systému IFIS a ISKAM:

nájemní smlouvy na pronájem bytů,
nájemní smlouvy nebytových prostor,
předávací protokoly bytů a nebytových prostor.
Zpracovává kamerové záznamy osob pohybujících se v areálu spravovaném
Organizací.

Podrobnosti viz příloha č. 2.

Odpovídá za: Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Skartování všech tištěných dokumentů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.12. Technické oddělení

Odpovědná osoba: Vedoucí Technického oddělení.

Eviduje a zpracovává: Osobní údaje zaměstnanců a dodavatelů v elektronických souborech, ve služebních mobilních telefonech a tabletech a osobní údaje ubytovaných osob v systému ISKAM, a tištěných dokumentech:

záznamy o školení PO,

záznamy o školení BOZP,

evidence odpracovaných hodin pracovníků údržby,

žádanky a objednávky,

servisní smlouvy,

objednávky,

dodavatelské smlouvy,

odběratelské smlouvy,

seznam klíčů,

evidence závad nahlášených ubytovanými osobami.

Podrobnosti viz příloha č. 2.

Odpovídá za: Bezpečnost, úplnost, aktuálnost a integritu osobních údajů v elektronických souborech, ve služebních mobilních telefonech, tabletech a tištěných dokumentech. Dodržení předepsaného rozsahu osobních údajů evidovaných v elektronických souborech ve služebním mobilním telefonu a tištěných dokumentech a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Smazání všech záznamů v elektronických souborech ve služebním mobilním telefonu a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potenciálních hrozeb narušení bezpečnosti osobních údajů.

6.13. Koleje a hotel VŠE

Odpovědné osoby: Vedoucí jednotlivých kolejí a hotelu pod správou Organizace.

Eviduje a zpracovává: Osobní údaje studentů VŠE, studentů jiných VŠ a zahraničních studentů, hotelových hostů, hotelových hostů-cizinců a potenciálních hotelových hostů v informačních systémech ISKAM a BOOKOLO a tištěných dokumentech. Zpracovává údaje o studentech VŠE v informačním systému InSIS. Eviduje a zpracovává osobní údaje zaměstnanců, návštěv, dodavatelů a odběratelů v tištěných dokumentech, elektronických souborech a e-mailech a v kamerových záznamech:

smlouva o ubytování,

dodatek smlouvy o ubytování,

doklad pro cizineckou polici,

kolejní průkaz,
formulář při odchodu,
doklad o zaplacení kolejného,
evidence návštěv,
nájemní smlouvy,
evidence odběratelů,
kontakty na zaměstnance hotelu a kolejí,
domovní kniha,
přihlašovací lístek.

Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v informačních systémech ISKAM a BOOKOLO a osobních údajů v tištěných dokumentech, elektronických souborech, služebních mobilních telefonech a e-mailech.

Dodržení předepsaného rozsahu osobních údajů evidovaných v jím spravovaných informačních systémech a tištěných dokumentech, elektronických souborech, služebních mobilních telefonech a e-mailech a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Smazání všech záznamů v informačních systémech a skartování tištěných dokumentů obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potencionálních hrozeb narušení bezpečnosti osobních údajů.

6.14. Menzy

Odpovědná osoba: Nájemce jednotlivých menz ve správě Organizace. Provozní oddělení

Eviduje a zpracovává: Osobní údaje studentů VŠE, studentů jiných VŠ, zahraničních studentů, zaměstnanců a ostatních stravovaných osob v informačním systému KREDIT. Podrobnosti viz příloha č. 2.

Odpovídá za: Pořízení, bezpečnost, úplnost aktuálnost a integritu osobních údajů v informačním systému KREDIT.

Dodržení předepsaného rozsahu osobních údajů evidovaných informačním systémem KREDIT a za dodržení oprávněné doby uchování osobních údajů dle přílohy č. 2.

Provádění pravidelné kontroly, jedenkrát za rok, oprávněné doby uchování osobních údajů, a rozsahu osobních údajů, které eviduje a zpracovává.

Smazání všech záznamů v informačním systému KREDIT obsahujících osobní údaje subjektů údajů po uplynutí zákonné doby pro jejich evidenci a archivaci.

Za včasnou identifikaci případného bezpečnostního incidentu.

Za identifikaci potencionálních hrozeb narušení bezpečnosti osobních údajů.

7. Způsoby zabezpečení osobních údajů a eliminace rizik bezpečnostních incidentů

7.1. Principy zabezpečení tištěných dokumentů

Tištěné dokumenty obsahující osobní údaje subjektů údajů nesmí nikdy zůstat volně přístupny za nepřítomnosti osoby odpovědné za jejich bezpečnost, viz kapitola 6. tohoto vnitřního předpisu, (princip čistého stolu).

Tištěné dokumenty obsahující osobní údaje subjektů údajů spravované odděleními dle kapitoly 6. tohoto vnitřního předpisu jsou umístěny v uzamykatelné místnosti příslušného oddělení, do které nemají přístup jiní zaměstnanci Organizace a v uzamykatelné skříni nebo šuplíku umístěném v této místnosti. Klíče od této místnosti a klíče od skříně/šuplíku mají pouze oprávnění zaměstnanci daného oddělení.

Hospodaření s klíči je upraveno Směrnicí VŠE SR 02/2021 „Ochrana a ostraha majetku VŠE v Praze a postup při ztrátách/nálezech“ a Příkazem ředitele SÚZ VŠE č. 1/2021 „Ochrana a ostraha majetku“.

V době nepřítomnosti oprávněných osob v dané místnosti musí být všechny dokumenty obsahující osobní údaje subjektů údajů umístěny v uzamčené skříni a daná místnost musí být zamčená, popř. musí být aktivováno pohybové čidlo.

7.2. Principy zabezpečení elektronických souborů

Elektronické soubory obsahující:

7.2.1.osobní údaje:

- jsou v souladu s kapitolou 6. tohoto vnitřního předpisu a v souladu s Analyzátozem osobních údajů (Příloha č. 2) uloženy na uložišti pod správou Centra informatiky VŠE s označením ONE DRIVE. Přístup k daným souborům je omezen pouze na oprávněné osoby a zároveň jsou synchronizovány na počítači s profilem VŠE s přístupem omezeným na konkrétní osobu. Za bezpečnost takto nastaveného uložště ONE DRIVE odpovídá Centrum informatiky VŠE.
- nesmí být uloženy na žádných externích discích nebo jiných uložštích dat ani na žádných počítačích mimo správu VŠE nebo na mobilních telefonech či na jiných mobilních zařízeních.

7.2.2.kamerové záznamy:

jsou uloženy na serveru v uzamykatelné místnosti Organizace, do které má přístup pouze oprávněná osoba. Za bezpečnost tohoto serveru, za jeho odolnost proti vnějším i vnitřním útokům, za jeho zálohování a případnou obnovu dat a za integritu na něm uložených dat odpovídá Organizace.

7.3. Principy použití a zabezpečení počítačů Organizace a služebních mobilních telefonů

Počítače organizace, stolní i notebooky, jsou chráněny antivirovým programem a firewallem v souladu s příkazem rektora PR 01/2007 „Provozování a využívání výpočetní techniky a počítačové sítě Vysoké škola ekonomické v Praze“.

Služební mobilní telefony musí být chráněny přístupovým heslem proti neoprávněnému použití třetí stranou. Usínání mobilních telefonů a jejich automatické chránění heslem nesmí být nastaveno na delší čas než 1 minuta.

V mobilních telefonech mohou být evidovány osobní údaje pouze v minimálním rozsahu a to jméno, příjmení, název organizace, číslo telefonu/mobilního telefonu, e-mailová adresa a doručovací adresa daného subjektu údajů.

7.4. Principy tvorby a správy přístupových hesel

Principy pro tvorbu a správu hesel do počítačů Organizace a do informačních systémů jsou upraveny příkazem rektora VŠE PR 07/2018 „Pravidla provozování a využívání universitního informačního systému Vysoké školy ekonomické v Praze“.

7.5. Principy ochrany a hierarchizace přístupů do informačních systémů

Principy ochrany a přidělování přístupových práv do informačních systémů jsou upraveny příkazem rektora VŠE PR 07/2018 „Pravidla provozování a využívání universitního informačního systému Vysoké školy ekonomické v Praze“.

Rozsah přístupových práv do jednotlivých informačních systémů pro zaměstnance Organizace schvaluje ředitel Organizace na návrh příslušného vedoucího oddělení.

7.6. Principy zabezpečení informačních systémů

Všechny informační systémy, kromě informačního systému **BOOKOLO** a **Kamerového systému**, jsou provozovány na serverech Centra informatiky VŠE. Centrum informatiky VŠE rovněž odpovídá za jejich bezpečnost proti vnějším i vnitřním útokům, za jejich zálohování a případnou obnovu dat a za integritu dat na nich uložených.

Informační systémy **ISKAM**, **BOOKOLO**, **KREDIT** a **Kamerový systém** jsou provozovány Organizací, která má na jejich údržbu a aktualizaci uzavřenou smlouvu s jejich dodavatelem včetně smlouvy o zpracování osobních údajů.

Centrum informatiky VŠE odpovídá:

- za provoz, údržbu a aktualizaci ostatních informačních systémů využívaných Organizací,
- za vnitřní přenos dat Kamerového systému Organizace.

Viz též příkaz rektora VŠE PR 07/2018, „Pravidla provozování a využívání univerzitního informačního systému Vysoké školy ekonomické v Praze“.

7.7. Principy využití elektronické pošty pro přenos osobních údajů

Pro přenos osobních údajů a dokumentů s osobními údaji elektronickou poštou je využívána pouze vnitřní elektronická pošta Organizace souladu s SR 4/2019 „Pravidla provozu elektronické pošty na Vysoké škole ekonomické v Praze“. Je zakázáno posílat osobní údaje a dokumenty obsahující osobní údaje na soukromé e-mailové adresy zaměstnanců.

Pro předávání osobních údajů a dokumentů obsahujících osobní údaje externím zpracovatelům, se kterými je uzavřena smlouva o zpracování je zásadně používána e-mailová adresa dohodnutá ve smlouvě o zpracování.

E-maily obsahující osobní údaje nebo v přílohách elektronické soubory s osobními údaji jsou mazány nejpozději po 5-ti letech.

7.8. Předávání tištěných dokumentů obsahujících osobní údaje uvnitř Organizace

Tištěné dokumenty obsahující osobní údaje jsou uvnitř organizace zásadně předávány buď osobně nebo v zalepené obálce se jménem osoby, které jsou určeny, prostřednictvím k tomuto účelu určených schránek Organizace.

8. Systém testování přijatých opatření na eliminaci rizik

Za testování jednotlivých opatření na eliminaci rizik bezpečnostního incidentu je v rámci správy ostatních informačních systémů využívaných organizací odpovědno Centrum informatiky VŠE.

Za testování odolnosti informačních systémů ISKAM a BOOKOLO, KREDIT a Kamerového systému proti bezpečnostním incidentům je odpovědna Organizace ve spolupráci s jejich dodavatelem.

Za testování odolnosti centrálního úložiště dat ONE DRIVE proti bezpečnostním incidentům je odpovědno Centrum informatiky VŠE.

Testování odolnosti proti bezpečnostním incidentům vzdáleného přístupu do počítačové sítě VŠE je odpovědno Centrum informatiky VŠE.

Všechna testování se v součinnosti s Centrem informatiky VŠE provádí alespoň jedenkrát do roka.

O provedeném testování provede Garant zpracování osobních údajů písemný záznam.

Testování jsou vždy provedena neprodleně, pokud byla odhalena potenciální hrozba bezpečnostního incidentu.

9. Principy kopírování dokumentů s osobními údaji

Kopírování tištěných i elektronických dokumentů obsahujících osobní údaje je zakázáno.

Výjimku pro řádně definovaný účel a předem stanovené období může písemně povolit pouze ředitel Organizace. Dokument musí být vždy označen jako KOPIE.

O provedené kopii musí být veden záznam. V záznamu musí být uvedeny informace o smazání/skartování kopie po uplynutí doby schválené pro její použití.

10. Způsoby zabezpečení provozoven

Administrativní a správní centrum Organizace (hlavní provozovna Organizace) je umístěno v Centru kolejí Jarov (CKJ).

V areálu Kampusu Jarov působí vnější ostraha objektů. Areál je chráněn kamerovým systémem. Vstup do hlavní provozovny Organizace je neustále uzamčen.

Evidenci nekopírovatelných klíčů a přístupových karet do hlavní provozovny Organizace vede určený pracovník Technického oddělení.

Vstup návštěv do hlavní provozovny Organizace je možný jen po ohlášení se příslušnému zaměstnanci přes dveřní komunikační systém, který si návštěvu vyzvedne u vstupních dveří a během pobytu v hlavní provozovně Organizace ji doprovází. Volný pohyb cizích osob v prostorách hlavní provozovny Organizace je zakázán.

Jednotlivé kanceláře hlavní provozovny Organizace jsou uzamykatelné klíčem, který není volně kopírovatelný. Evidenci přidělených klíčů vede určený pracovník Technického oddělení. Klíče k jednotlivým kancelářím jsou přidělovány na návrh vedoucího oddělení. Universální klíč od všech kanceláří má přidělen ředitel Organizace a vedoucí Technického oddělení.

Vstup na jednotlivé koleje je možný jen za použití karty přístupového systému. Vstupy na jednotlivé koleje jsou hlídány kamerovým systémem s možností zpětného dohledání po dobu 5 dní.

Recepce s 24 hodinovým provozem jsou na University hotelu, Eislerově koleji, koleji Blanice a koleji Vltava.

11. Principy zálohování, archivace a obnovy osobních údajů

Tištěné dokumenty nejsou zálohovány.

Za zálohování a případnou obnovu dat informačních systémů a dat uložených na uložišti ONE DRIVE je odpovědné Centrum informatiky VŠE.

12. Zásady skartace tištěných i elektronických médií s osobními údaji

Tištěné dokumenty jsou skartovány po uplynutí doby pro jejich oprávněnou evidenci na k tomu určeném skartovacím zařízení, popř. vybranou firmou.

Na případnou skartaci všech zařízení s uloženými elektronickými daty a skartaci nosičů elektronických dat je najímána odborná firma.

13. Vyřizování požadavků subjektů údajů

Požadavky a námítky subjektů údajů v souladu s Nařízením ve spolupráci s DPO VŠE vyřizuje Garant zpracování osobních údajů. Jedná se o tyto požadavky:

13.1. Oprava osobních údajů.

13.2. Výmaz osobních údajů.

13.3. Vypořádání námitek subjektů údajů.

13.4. Omezení zpracování osobních údajů.

13.5. Zajištění přístupu subjektů údajů k osobním údajům a přenos osobních údajů jinému správci.

14. Proces vedení záznamů o činnosti zpracování osobních údajů

Za vedení Registru zpracování osobních údajů je odpovědný DPO VŠE.

15. Principy profilování

Organizace neprovádí profilování subjektů údajů.

16. Zásady předávání osobních údajů do zahraničí

Organizace nepředává osobní údaje subjektů údajů do zahraničí.

V případě požadavku subjektu údajů na předání jeho osobních údajů příslušnému správci do zahraničí bude toto uskutečněno jedině po jeho výslovném souhlasu v souladu s Nařízením.

17. Systém odhalování bezpečnostních incidentů

Za systém odhalování bezpečnostních incidentů v oblasti dat jednotlivých informačních systémů uložených na serverech Centra informatiky VŠE a na uložišti ONE DRIVE je odpovědné Centrum informatiky VŠE.

Za odhalování bezpečnostních incidentů uvnitř Organizace je odpovědný každý zaměstnanec Organizace v souladu s kapitolou 6. tohoto vnitřního předpisu.

18. Systém informování Úřadu a subjektů údajů o bezpečnostních incidentech

Za včasné podání informací dozorovému úřadu o případném bezpečnostním incidentu (do 72 hodin) je v součinnosti s DPO VŠE odpovědný Garant zpracování osobních údajů.

Záznamy o případných bezpečnostních incidentech vede DPO VŠE.

19. Principy motivačního systému k dodržování zásad bezpečnosti osobních údajů

Odměňování všech zaměstnanců Organizace uvedených jako osoby odpovědné za evidenci a zpracování osobních údajů v kapitole 6. tohoto vnitřního předpisu je ze 100 % závislé na skutečnosti, že během období rozhodného pro výplatu odměn nedošlo k bezpečnostnímu incidentu. To znamená, že jejich odměny, na které mají jinak v Organizaci nárok, mohou být na základě rozhodnutí ředitele Organizace v případě bezpečnostního incidentu kráceny až o 100 %.

Ředitel Organizace může udělit mimořádnou odměnu zaměstnanci, který upozorní na potenciální riziko bezpečnostního incidentu, popř. odhalí bezpečnostní incident.

20. Definice odpovědnosti zaměstnanců za bezpečnost osobních údajů

Všichni zaměstnanci Organizace jsou odpovědní za bezpečnost osobních údajů evidovaných a zpracovávaných v Organizaci v míře odpovídající jejich pracovnímu zařazení.

Všichni zaměstnanci Organizace jsou povinni neprodleně hlásit všechny jimi zjištěné bezpečnostní incidenty, a to včetně jimi identifikovaných potenciálních bezpečnostních hrozeb. Odpovědné osobě uvedené v kapitole 3. tohoto předpisu.

21. Pravidla pro používání soukromých elektronických zařízení

Používání soukromých elektronických zařízení zaměstnanců podniku, jako jsou soukromé mobilní telefony, soukromé tablety, soukromé notebooky nebo jiná soukromá zařízení nebo soukromá elektronická média pro elektronické uchování a zpracování osobních údajů je zakázáno.

22. Principy práce z domova

Práce z domova, v souladu s příkazem ředitele č. 5/2021, je umožněna pouze vybraným zaměstnancům na základě souhlasu ředitele Organizace. Práce z domova je povolena pouze přes VPN nastavenou a spravovanou Centrem informatiky VŠE a na zařízeních Organizace.

Všichni pracovníci s možností práce z domova musí dbát na bezpečnost osobních údajů a nesmí ponechat své počítače připojené k počítačové síti Organizace/VŠE přes VPN v době své nepřítomnosti.

Zabezpečení počítačů používaných pro práci z domova musí odpovídat standardům uvedeným v příkazu rektora VŠE PR 01/2007 „Provozování a využívání výpočetní techniky a počítačové sítě Vysoké školy ekonomické v Praze“.

Vzdálený přístup externím spolupracovníkům a dodavatelům je umožněn pouze na základě podpisu smlouvy o zpracování v souladu s Nařízením a pouze přes VPN nastavenou a spravovanou Centrem informatiky VŠE.

23. Pravidla používání elektronických zařízení a médií s osobními údaji mimo prostory provozovny

Mimo prostory provozovny Organizace je povoleno používat pouze služební mobilní telefony a služební notebooky přidělené Organizací. Služební mobilní telefony a notebooky přidělené Organizací musí být chráněny heslem v případě jejich zapínání a zároveň v případě jejich usnutí v souladu s příkazem rektora VŠE PR 01/2007 „Provozování a využívání výpočetní techniky a počítačové sítě Vysoké školy ekonomické v Praze“ tak, aby bylo zabráněno zneužití přes ně přístupných osobních údajů třetí stranou.

24. Zásady školení zaměstnanců v oblasti bezpečnosti osobních údajů

Všichni zaměstnanci Organizace jsou minimálně jedenkrát ročně proškoleni v zásadách ochrany osobních údajů stanovených tímto vnitřním předpisem v míře odpovídající jejich pracovnímu zařazení. O tomto proškolení je veden záznam podle přílohy č. 1 tohoto vnitřního předpisu.

V případě významných legislativních změn v oblasti ochrany osobních údajů proběhne školení všech zaměstnanců Organizace neprodleně poté, co bude znám úplný charakter těchto změn a co tyto změny vstoupí v platnost.

Za školení zaměstnanců podniku odpovídá Garant zpracování osobních údajů.

Příloha č. 2
Analyzátor osobních údajů – soubor v EXCELU.
Pouze pro vnitřní potřebu SÚZ VŠE

Příloha č. 3

Registr zpracování osobních údajů

Viz soubor v Excelu „VŠE SÚZ_CINNOSTI_ZPRACOVANI.xlsx“

Souhlas se zpracováním osobních údajů¹

udělený podle Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů

Já, **jméno příjmení**, narozený dne **XX. XX. XXXX** bytem **ulice čp/čo, PSČ, obec**, uděluji dobrovolně souhlas se zpracováním mých osobních údajů správci údajů:

Název: **Vysoká škola ekonomická v Praze - Správa účelových zařízení**

IČ: **61384399**

Sídlo: **Jeseniova 2769/208, 130 00 Praha 3**

Kontaktní osoba: **Ing. Jan Zavřel, e-mail: gdpr-suz@vse.cz, telefon: 224 09 2118**

Pověřenec pro ochranu osobních údajů: **RNDr. Karel Nenadál, e-mail: dpo@vse.cz, telefon: 224 09 5710**

ke zpracování mých osobních údajů v rozsahu **[jméno příjmení, e-mail, telefon, adresa,.....doplnit dle potřeby]**;

za účelem **[doplnit popis účelu jednoduchou a srozumitelnou řečí]**;

na dobu **[určit dobu, po kterou bude souhlas platit, nebo způsob jak bude stanovena]**.

- Nesouhlasím s předáním mých osobních údajů třetí straně.²
- Souhlasím s předáním mých osobních údajů třetí straně. **[uvést komu (identifikovat) a za jakým účelem budou osobní údaje předány, zvláště pečlivě a srozumitelně je třeba vysvětlit v případě úmyslu správce předat osobní údaje mimo EU]**.

Jsem si vědom že:

- tento souhlas můžu kdykoliv odvolat **[uvést způsob jak může být souhlas odvolán]**;
- mám právo na bezplatný přístup k mým osobním údajům **[uvést způsob jak]**;
- mám právo získat všechny mé osobní údaje v obvyklém strojově čitelném formátu **[uvést způsob jak]**;
- mám právo požádat o převod mých osobních údajů jinému správci osobních údajů podle mé volby **[uvést způsob jak]**;
- mám právo na opravu mých osobních údajů **[uvést způsob jak]**;
- mám právo požádat o výmaz mých osobních údajů **[uvést způsob jak]**;
- mám právo požádat o omezení zpracování mých osobních údajů **[uvést způsob jak]**;
- mám právo vznést námitku proti prováděnému zpracování mých osobních údajů **[uvést způsob jak]**;
- v otázkách zpracování mých osobních údajů mám právo kontaktovat správce mých osobních údajů **[uvést způsob jak]**;
- v případě, že se domnívám, že mé osobní údaje jsou zpracovávány v rozporu s právními předpisy, mám právo obrátit se na správce s žádostí o zjednání nápravy **[uvést způsob jak]**;
- v oprávněných případech mám právo podat stížnost přímo u Úřadu pro ochranu osobních údajů (<https://www.uoou.cz/>) – například e-mailem na posta@uoou.cz;
- beru na vědomí, že správce bude tento můj souhlas archivovat pro účely plnění své právní povinnosti být schopen doložit, že jsem mu tento souhlas ke zpracování osobních údajů udělal.

V _____ dne _____

podpis _____

¹ **Navržený dokument musíte upravit na konkrétní podmínky ve vašem podniku/organizaci. Bez dalších úprav na konkrétní podmínky ve vašem podniku/organizaci jej nelze použít!**

² Označte odpovídající políčko dle své volby křížkem

Legenda:

Datum porušení	Uveďte datum, kdy došlo k porušení bezpečnosti osobních údajů
Popis porušení zabezpečení osobních údajů	Doplňte popis porušení bezpečnosti osobních údajů; např. odcizení přihlašovacích údajů, ztráta nosičů osobních údajů, atd.]
Doba trvání porušení	Doplňte dobu, po kterou trvalo porušení bezpečnosti osobních údajů (v časových jednotkách minuty, hodiny, dny,...)
Kategorie subjektů údajů	Subjektem údajů se rozumí identifikovatelná fyzická osoba, které se osobní údaj týká. Kategorii subjektů údajů mohou být např. zaměstnanci, uchazeči o zaměstnání, zákazníci (fyzické osoby), dodavatelé (fyzické osoby), osoby pohybující se v areálu podniku atd.
Dopady porušení zabezpečení osobních údajů	Doplňte účinky (dopady) porušení bezpečnosti osobních údajů; např. přístup neoprávněných osob k osobním údajům, odcizení osobních údajů, smazání osobních údajů, přepsání osobních údajů atd.
Dopad na práva a svobody subjektů údajů	Doplňte míru rizika plynoucího z porušení bezpečnosti osobních údajů pro dotčené fyzické osoby. Pokud je riziko nepravděpodobné, není nutné porušení hlásit dozorovému úřadu. V případě vysokého rizika je nutné informovat o porušení též subjekty údajů.
Přijatá nápravná opatření	Doplňte popis přijatých nápravných opatření.

Informace o zpracování osobních údajů zaměstnance³

Zaměstnavatel - Správce

Název: Vysoká škola ekonomická v Praze – Správa účelových zařízení

IČ: 61384399

Sídlo: Jeseniova 2769/208, 130 00 Praha 3

Kontaktní osoba: Ing. Jan Zavřel, e-mail: gdpr-suz@vse.cz, telefon: 224 09 2118

Pověřenec pro ochranu osobních údajů: RNDr. Karel Nenadál, e-mail: dpo@vse.cz, telefon: 224 09 5710

1. Účel a rozsah zpracování osobních údajů

V souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (dále Nařízení) Správce zpracovává osobní údaje zaměstnanců, které jsou přiměřené, relevantní a omezené na nezbytný rozsah. Osobní údaje zpracovává za účelem vedení personální a mzdové agendy a za účelem dodržení svých povinností podle obecně závazných právních předpisů.

Osobní údaje zaměstnance budou zpracovávány po dobu trvání pracovního poměru zaměstnance a dále uchovávány po dobu stanovenou obecně závaznými právními předpisy.

Správce je oprávněn předat osobní údaje zaměstnanců účetním a daňovým poradcům, kteří budou osobní údaje zpracovávat pro Správce jako jeho zpracovatelé.

2. Práva zaměstnance

Zaměstnanec má právo požadovat od Správce přístup ke svým osobním údajům (viz čl. 15 Nařízení), jejich opravu nebo výmaz (viz čl. 16 nebo čl. 17 Nařízení), popř. omezení zpracování (viz čl. 18 Nařízení). Zaměstnanec má dále právo vznést námitku proti zpracování (viz čl. 21 Nařízení).

Pokud se zaměstnanec domnívá, že jsou jeho osobní údaje zpracovávány v rozporu s právními předpisy, má právo obrátit se na Správce s žádostí o zjednání nápravy. Jestliže bude žádost zaměstnance shledána oprávněnou, Správce neprodleně odstraní závadný stav. Tím není dotčena možnost zaměstnance podat stížnost přímo u Úřadu pro ochranu osobních údajů.

Převzal dne:

.....

podpis zaměstnance

³ Navržený dokument musíte upravit na konkrétní podmínky ve vašem podniku/organizaci. Bez dalších úprav na konkrétní podmínky ve vašem podniku/organizaci jej nelze použít!

Informace o zpracování osobních údajů dodavatelů a zákazníků⁴

Správce

Název: Vysoká škola ekonomická v Praze - Správa účelových zařízení

IČ: 61384399

Sídlo: Jeseniova 2769/208, 130 00 Praha 3

Kontaktní osoba: Ing. Jan Zavřel, e-mail: gdpr-suz@vse.cz , telefon: 224 09 2118

Pověřenec pro ochranu osobních údajů: RNDr. Karel Nenadál, e-mail: dpo@vse.cz, telefon: 224 09 5710

1. Účel a rozsah zpracování osobních údajů

V souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (dále Nařízení) Správce při plnění smlouvy uzavřené se zákazníkem - subjektem údajů - zpracovává osobní údaje subjektu údajů, které jsou přiměřené, relevantní a omezené na nezbytný rozsah a po dobu, která vyplývá z účelu jejich zpracování.

1.1 Osobní údaje Správce zpracovává za účelem plnění smlouvy až do doby zániku závazků ze smlouvy a to včetně záruční doby.

1.2 Osobní údaje Správce zpracovává za účelem plnění svých právních povinností vyplývajících z obecně závazných právních předpisů, (např. povinnost Správce uchovávat účetní a daňové doklady) a to po dobu trvání příslušné právní povinnosti Správce.

1.3 Osobní údaje správce zpracovává pro účely svých oprávněných zájmů, pro účely přímého marketingu - zaslání obchodních sdělení - a to do uplynutí 2. kalendářního roku následujícího po zániku závazků ze smlouvy nebo do doby než subjekt údajů vyjádří svůj nesouhlas s tímto druhem zpracování svých osobních údajů.

Nejpozději do konce kalendářního měsíce následujícího po uplynutí doby zpracování budou příslušné osobní údaje, u kterých pominul účel jejich zpracování, zlikvidovány nebo anonymizovány tak, že se s nimi nebudou moci seznámit neoprávněné osoby.

Správce je oprávněn předat osobní údaje příjemcům, se kterými uzavřel smlouvu o zpracování osobních údajů a kteří budou pro Správce zpracovávat osobní údaje jako jeho zpracovatelé. Jedná se o *[Doplnit příjemce - zpracovatele. Doplnit případně informace o úmyslu Správce předávat osobní údaje do třetí země (tj. mimo EU nebo EHP) nebo mezinárodní organizaci včetně doplňujících informací podle čl. 13 odst. 1 písm. f) GDPR]*

3. Práva subjektu údajů

Subjekt údajů má právo požadovat od Správce přístup ke svým osobním údajům (viz čl. 15 Nařízení), jejich opravu nebo výmaz (viz čl. 16 nebo čl. 17 Nařízení), popř. omezení zpracování (viz čl. 18 Nařízení). Subjekt údajů má dále právo vznést námitku proti zpracování (viz čl. 21 Nařízení).

Pokud se subjekt údajů domnívá, že jsou jeho osobní údaje zpracovávány v rozporu s právními předpisy, má právo obrátit se na Správce s žádostí o zjednání nápravy. Jestliže bude žádost subjektu údajů shledána oprávněnou, Správce neprodleně odstraní závadný stav. Tím není dotčena možnost subjektu údajů podat stížnost přímo u Úřadu pro ochranu osobních údajů.

⁴ Navržený dokument musíte upravit na konkrétní podmínky ve vašem podniku/organizaci. Bez dalších úprav na konkrétní podmínky ve vašem podniku/organizaci jej nelze použít!

Příslušné odstavce této informace mohou být součástí například smlouvy o dílo, nebo jiného typu smlouvy.