

ZÁZNAMY O ČINNOSTECH ZPRACOVÁNÍ

Správce:

INT Group s.r.o., se sídlem Uherský Brod, Jabloňová 2381, PSČ 68801, IČ: 29283230

kontaktní údaje správce:

Adresa: sídlo (viz shora), e-mail: info@intgroup.cz, tel: 602 725 565

Agenda (odpovědné oddělení)	Kategorie subjektu údajů	Osobní údaje	Účel zpracování	Právní základ pro zpracování a) souhlas nebo smlouva se subjektem b) nezbytnost pro plnění smlouvy c) nezbytnost pro plnění právní povinnosti správce d) nezbytnost pro ochranu životně důležitých zájmů subjektu osobních údajů e) nezbytnost pro splnění úkolu prováděného ve veřejném zájmu f) oprávněné zájmy správce	Zdroj osobních údajů	Příjemci osobních údajů	Předávání údajů třetí země nebo mezinárodní organizaci	Doba uchování	Jak se poskytují oprávněným subjektům údajů předepsané informace?	Popis technických a organizačních bezpečnostních opatření
1	Personální	Zaměstnanci	zejména: • jméno, příjmení (rod. příjmení), RČ, datum a místo narození • bydliště • rodinný stav • státní příslušnost • počet vyživovacích dětí • vzdělání, titul • informace o mzdě • číslo bankovního účtu • kontaktní údaje (tel. číslo, e-mail) • zdravotní pojišťovna • zdravotní stav • fotografie a obrazové záznamy	• pro uzavření a plnění pracovněprávních a souvisejících smluv • plnění právních povinností, které se na správce vztahují, zejm. v oblasti práva pracovního, sociálního zabezpečení, daňového (např. pracovněprávní evidence, účetní evidence, vyplácení mzdy a plateb zdravotního pojištění, pojištění na sociální zabezpečení, daní) daňové povinnosti správce (vůči pojišťovám, finanční správě, ČSSZ, apod.) • benefitů pro zaměstnance • zjednodušení kontaktu a usnadnění komunikace se zaměstnancem • ochrana oprávněných zájmů správce (ochrana majetku, života a zdraví, tj. zejména sledování dostupnosti únikových cest, předcházení, odhalování a prokazování protiprávního jednání, odhalování vzniku živelných událostí a jiných škod, zajištění celkové bezpečnosti objektu)	• subjekt údajů • veřejně přístupné zdroje a databáze • kamerový systém správce	• zdravotní pojišťovny • orgány sociálního zabezpečení • finanční úřady • zpracovatelé (účetní a daňový poradci, poradci BOZP a PO, IT, bezpečnostní služba, závodní lékařská péče) • Policie ČR a orgány činné v trestním řízení (kamerový systém) • další orgány veřejné správy	• NE	• po dobu trvání pracovního poměru a dále po skončení pracovního poměru po dobu uchování stanovenou obecně závaznými právními předpisy • dle kapacity úložiště, max. 5 dnů (pro záznam z kamerového systému)	• poučení dle pracovní smlouvy • poučení zaměstnance o zpracování a ochraně osobních údajů zaměstnavatelem • v odpovědích na žádosti subjektů údajů • tabulky s informací o monitorování prostor	• k osobním údajům mají přístup pouze oprávněné osoby; • osobní údaje na pevných nosičích (listiny) jsou v uzamykatelných skříních; • osobní údaje v počítačích a na jiných paměťových nosičích jsou chráněny pravidelně se obměňujícím heslem; server je nepřístupný nepovolaným osobám (přístup k serveru je chráněn - uzamčen); • jednotlivé kanceláře jsou uzamykány, přístup do prostor s osobními údaji je zabezpečen alarmem s napojením na pult centrální ochrany; • kamerový systém je ovládán ze zabezpečeného jednotného místa (velína), do kterého mají přístup jen povolané osoby; • IT systém je standardní, spolehlivý, chráněn antivirem; přístup do IT je omezen dle nastavených manažerských rolí. IT systém je pravidelně testován a udržován; • s externími zpracovateli osobních údajů jsou uzavřeny smlouvy o zpracování osobních údajů; • osobní údaje jsou ve stanovených lhůtách likvidovány.
2	Recruitment	Potenciální zaměstnanci	• údaje v životopise	• pro uzavření pracovněprávních a souvisejících smluv (potřeba nového zaměstnance)	• subjekt údajů	• NE	• NE	• do odvolání souhlasu	• v poučení subjektu údajů • v odpovědích na žádosti subjektů údajů	• k osobním údajům mají přístup pouze oprávněné osoby; • osobní údaje na pevných nosičích (listiny) jsou v uzamykatelných skříních; • osobní údaje v počítačích a na jiných paměťových nosičích jsou chráněny pravidelně se obměňujícím heslem; server je nepřístupný nepovolaným osobám (přístup k serveru je chráněn - uzamčen); • jednotlivé kanceláře jsou uzamykány, přístup do prostor s osobními údaji je zabezpečen alarmem s napojením na pult centrální ochrany; • kamerový systém je ovládán ze zabezpečeného jednotného místa (velína), do kterého mají přístup jen povolané osoby; • IT systém je standardní, spolehlivý, chráněn antivirem; přístup do IT je omezen dle nastavených manažerských rolí. IT systém je pravidelně testován a udržován; • s externími zpracovateli osobních údajů jsou uzavřeny smlouvy o zpracování osobních údajů; • osobní údaje jsou ve stanovených lhůtách likvidovány.
3	Kamerový systém se záznamem	1) Zaměstnanci 2) Kdokoliv (smluvní partneři)	• obrazové záznamy, fotografie	• ochrana oprávněných zájmů správce (ochrana majetku, života a zdraví, tj. zejména sledování dostupnosti únikových cest, předcházení, odhalování a prokazování protiprávního jednání, odhalování vzniku živelných událostí a jiných škod, zajištění celkové bezpečnosti objektu)	• kamerový systém správce	• Policie ČR a orgány činné v trestním řízení • bezpečnostní služba	• NE	• dle kapacity úložiště, max. 5 dnů	• tabulky s informací o monitorování prostor • v odpovědích na žádosti subjektů údajů	• k osobním údajům mají přístup pouze oprávněné osoby; • osobní údaje na pevných nosičích (listiny) jsou v uzamykatelných skříních; • osobní údaje v počítačích a na jiných paměťových nosičích jsou chráněny pravidelně se obměňujícím heslem; server je nepřístupný nepovolaným osobám (přístup k serveru je chráněn - uzamčen); • jednotlivé kanceláře jsou uzamykány, přístup do prostor s osobními údaji je zabezpečen alarmem s napojením na pult centrální ochrany; • kamerový systém je ovládán ze zabezpečeného jednotného místa (velína), do kterého mají přístup jen povolané osoby; • IT systém je standardní, spolehlivý, chráněn antivirem; přístup do IT je omezen dle nastavených manažerských rolí. IT systém je pravidelně testován a udržován; • s externími zpracovateli osobních údajů jsou uzavřeny smlouvy o zpracování osobních údajů; • osobní údaje jsou ve stanovených lhůtách likvidovány.
4	Obchodní a smluvní	Smluvní partneři	zejména: • jméno a příjmení • firma • adresa sídla • IČ, DIČ • údaj o registraci k DPH • fakturační údaje (číslo bankovního účtu, kontaktní údaje (tel. číslo, e-mail) • banka, příp. údaj o zápisu do obchodního rejstříku • obrazový záznam (kamerový systém)	• pro uzavření a plnění pracovněprávních a souvisejících smluv • plnění právních povinností, které se na správce vztahují, zejm. v oblasti práva účetních, daňových • klíčové hospodářství • evidence kontaktních osob nájemních jednotek • ochrana oprávněných zájmů správce (ochrana majetku, života a zdraví, tj. zejména sledování dostupnosti únikových cest, předcházení, odhalování a prokazování protiprávního jednání, odhalování vzniku živelných událostí a jiných škod, zajištění celkové bezpečnosti objektu) • zaslání obchodních nabídek	• subjekt údajů • veřejně přístupné zdroje a databáze • kamerový systém správce	• zpracovatelé (účetní a daňový poradci, poradci BOZP a PO, IT, bezpečnostní služba) • orgány veřejné správy • Policie ČR a orgány činné v trestním řízení	• NE	• po dobu uchování stanovenou obecně závaznými právními předpisy • dle kapacity úložiště, max. 5 dnů (pro záznam z kamerového systému) • do odvolání souhlasu (zasílání obchodních sdělení)	• v poučení subjektu údajů • v odpovědích na žádosti subjektů údajů • tabulky s informací o monitorování prostor	• k osobním údajům mají přístup pouze oprávněné osoby; • osobní údaje na pevných nosičích (listiny) jsou v uzamykatelných skříních; • osobní údaje v počítačích a na jiných paměťových nosičích jsou chráněny pravidelně se obměňujícím heslem; server je nepřístupný nepovolaným osobám (přístup k serveru je chráněn - uzamčen); • jednotlivé kanceláře jsou uzamykány, přístup do prostor s osobními údaji je zabezpečen alarmem s napojením na pult centrální ochrany; • kamerový systém je ovládán ze zabezpečeného jednotného místa (velína), do kterého mají přístup jen povolané osoby; • IT systém je standardní, spolehlivý, chráněn antivirem; přístup do IT je omezen dle nastavených manažerských rolí. IT systém je pravidelně testován a udržován; • s externími zpracovateli osobních údajů jsou uzavřeny smlouvy o zpracování osobních údajů; • osobní údaje jsou ve stanovených lhůtách likvidovány.