Směrnice o informační bezpečnosti pro dodavatele společnosti HF-Czechforge a dodavatele společnostem koncernu Hammerwerk Fridingen GmbH

Tato směrnice doplňuje Všeobecné obchodní podmínky dodavatelské, upravující smluvní vztahy mezi dodavateli a společností HF-Czechforge s.r.o.

Zhotovitelem se pro účely této směrnice rozumí dodavatel zboží a služeb.

Zadavatelem/objednatelem se rozumí firma HF-Czechforge s.r.o., případně jiná ze společností koncernu Hammerwerk Fridingen GmbH, která zhotovitele pověřila dodávkou zboží či služby.

Zakázkou se rozumí dodávka zboží či služby na základě objednávky, smlouvy o dílo či jiného podobného zadání.

Dodávkami se rozumí dodávky zboží i služeb.

Pojem „Podnik dodavatele“ představuje veškeré zboží, procesy a systémy (včetně informačních systémů), data (včetně dat zákazníků), zaměstnance a lokace společnosti, které jsou dočasně pro realizaci dotčené zakázky používány nebo zpracovávány.

I.
Informační bezpečnost

1. Zhotovitel musí disponovat přiměřenými organizačními a technickými opatřeními, odpovídajícími současným standardům tak, aby si zajistil důvěru, autenticitu, integritu a disponibilitu svého dodavatelského podniku, jakož i svými dodávkám a výkonům. Zmíněná opatření by měla odpovídat obvyklým, používaných v příslušném oboru a měla by též přiměřeně odrážet Systém řízení bezpečnosti informací, a to v souladu se standardy, jako jsou ISO/IEC 27001 nebo IEC 62443 (pokud je lze použít).

   Zhotovitel umožní objednateli přístup do svých zařízení po příslušném nahlášení tak, aby se mohl přesvědčit o tom, že byla přijata vhodná technická a organizační opatření.
2. V celém areálu zadavatele je zakázáno bez předchozího písemného souhlasu vytvářet obrazové nebo zvukové záznamy jakéhokoliv druhu.
3. Pokud dodávky obsahují software, firmware nebo čipy:
   - provede dodavatel přiměřenou implementaci procesů a metod v souladu se standardy jako jsou ISO/IEC 27001 nebo IEC 62443, která je v příslušném oboru obvyklá, aby se zabránilo vzniku jakýchkoliv slabých míst, škodlivých kódů a bezpečnostně relevantních událostí v dodávkách a bylo je možné identifikovat, vyhodnotit a odstranit.
   - nabídne dodavatel pro časové období přiměřené doby existence dodávky servisní výkony, update, upgrade a jiné výkony povahy údržby a patches, aby mohlo dojít k odstranění slabých míst.
   - poskytne dodavatel soupis, z něhož bude možné zjistit, které komponenty software, obsažené v dodávce byly původem od třetích osob. Komponenty software třetích osob obsažené v dodávce musí být v okamžiku jejich dodání na úrovni odpovídající současným standardům.
   - je zadavatel oprávněn, avšak ne povinen, sám nebo prostřednictvím jím pověřené třetí osoby kdykoliv otestovat dodávky na přítomnost škodlivých kódů a slabých míst, přičemž je dodavatel povinen zadavateli v tomto směru poskytnout přiměřenou podporu.
4. Zhotovitel předá zadavateli kontakt na osobu pro témata informační bezpečnosti, dosažitelnou v obvyklém čase pracovní doby, po dobu trvání dodané služby, či používání dodaného zboží.

5. Zhotovitel zajistí taková opatření, aby svým zaměstnancům a subdodavatelům v rámci přiměřené doby uložil povinnosti, které odpovídají povinnostem obsaženým v této Směrnici.

II.
Zachovávání mlčenlivosti

1. Zhotovitel se zavazuje zachovat mlčenlivost o důvěrných nebo přísně důvěrných informacích a používat je výhradně pro účely zpracování zakázky. Toto platí též i po ukončení zakázky a vztahuje se na zaměstnance zhotovitele i jeho subdodavatele.
2. Za důvěrné mohou být považovány zejména následující informace a/nebo předměty (jednotlivě nebo v jejich celistvosti):
   - technické informace, obzvláště popisy výrobků, jejich funkčnosti a vývojových stádií, specifikace, náčrty, grafiky, výkresy a další příručky a technické znalosti;
   - informace o stávajících nebo budoucích právních vztazích dotýkajících se produktu, zejména uživatelská práva, licencování, přihlášení k patentování a vynálezy které jsou schopné patentování, užitné vzory, práva k průmyslovým vzorům nebo ochranným známkám, jakož i mnohá další práva;
   - informace o podnikatelské strategii, časové plány, cíle, nápady, plánované projekty, odbytové cesty jakož i obchodní data, zejména obraty a marže;
   - informace, se kterými přijde do styku zhotovitel v rámci opatření k servisním pracím nebo údržbě prováděných na zařízení/stroji nebo komponentech v rámci instalace a zprovoznění dodávek pro zadavatele;
   - IT-know-how, jako např. výbava, procesy, programy a licence, vývojová stádia, výměna dat, bezpečnostní zařízení a opatření.
3. Veškeré důvěrné informace, které objednatel poskytne zhotovitelovi zůstávají výhradním vlastnictvím objednatele.

III.
Ohlašovací povinnost

1. Události dotýkající se bezpečnosti informací musí být okamžitě hlášeny našemu pověřenci pro informační bezpečnost, a to na e-mailové adrese: *ismb@hammerwerk.de*. Nahlášeny budou údaje o škodní události, okamžitá opatření, příčiny a dlouhodobá opatření. Kontaktní osoba na straně zhotovitele bude následně bez zbytečných průtahů iniciovat proces k vyřešení události. *Příloha č. 1* této směrnice určuje rozsah ohlášení. Potenciálními incidenty mohou být např.
   - neúčinná bezpečnostní opatření, podezření ze ztráty dat, krádež dat;
   - porušení očekávaného zachování důvěrnosti informací;
   - chybná funkce software, která ohrožuje bezpečnost informací;
2. Zhotovitel umožní objednateli přístup do svých zařízení, aby se mohl přesvědčit o připravenosti realizovat vhodná technická a organizační opatření k zamezení takových událostí a k omezení vzniku škod v případě vzniku takové události.

IV.
Ochrana dat

1. Každá ze stran je povinna dodržovat zákonná ustanovení o ochraně dat, zejména Obecné nařízení EU o ochraně osobních údajů a dodržování těchto ustanovení uložit svým zaměstnancům.

2. Každá ze stran zpracovává pouze osobní údaje, které od druhé strany obdržela (např. jména a kontaktní data příslušných kontaktních osob), a to výhradně k naplnění příslušné zakázky. Prostřednictvím technických bezpečnostních opatření poskytuje těmto datům ochranu na úrovni současných standardů. Každá ze stran je povinna osobní údaje druhé strany vymazat, pokud jejich zpracování již není potřeba. Jakékoliv zákonné povinnosti o uchování osobních údajů zůstávají tímto nedotčeny.
3. Pokud by jedna ze stran v rámci realizace ujednání zpracovávala, resp. pracovala v zakázce s osobními údaji, uzavřou k tomuto smluvní strany ujednání o zpracovávání zakázky podle zákona o ochraně osobních údajů. Dodatečné zpracovávání pro vlastní účely je vyloučeno.

V.

Výměna dat

1. Zhotovitel se zavazuje používat postupy pro výměnu dat stanovené objednatelem, pokud je objednatel stanovil.

V Chebu, dne 9.12.2024

Ing. Jiří Strádal, jednatel v.r.
Ing. Petra Rančevová, finanční ředitelka v.r

Příloha č. 1

Formulář pro ohlášení události dotýkající se informační bezpečnosti

1. **Základní údaje o události**
   Zjištění události
   Datum:_____čas: _____
   Čas vzniku události, dotčený časový úsek:_____
   Postup zpracování dat:_____
   Odpovědný úsek/oddělení:_____
   Osoba odpovědná za událost:_____

Popis události

Dotčené systémy/objekty
Jak k události došlo
Jaké následky byly zjištěny

Reakce a stav systému

Jaké jsou příčiny události
Jaké jsou reakce/přijatá opatření na událost (rychlá opatření k nápravě a dlouhodobá opatření k zamezení možného opakování události)
Aktuální stav systému

2. **Údaje o události**
   2.1 Druh události:
   (možné příklady událostí např. ztráta důvěrnosti, krádež dat, zničení nebo zfalšování dat, předání dat neoprávněným osobám atd.)
   2.2 Kategorie informací/osobní údaje.
   2.3 Pravděpodobné následky/rizika poškození ochrany informací *(zde se uvedou možná rizika a následky dotčené situace).*
3. **Nařízená/provedená opatření k zjednání nápravy**
   3.1 Provedená opatření
   (Na tomto místě se popíší opatření, která byla provedena.)
   3.2 Další zamýšlená opatření
   (Na tomto místě se popíší ta opatření, jejichž zavedení je, na základě povahy události, dodatečně plánováno.)