NIS 2 ČL. 21 ODST. 2 PÍSM. D)

Dotazník pro dodavatele NIS 2

Otevřený dotazník pro posouzení dodavatelů podle NIS 2, ukotvený v právu EU

Profil dodavatele	16 polí
Bezpečnostní postupy	31 polí
Software jako služba (SaaS)	2 pole
Software u zákazníka (on-premise)	4 pole

U každé otázky je uveden její zdroj v právu EU: prováděcí nařízení (EU) 2024/2690, Technical Implementation Guidance agentury ENISA, obecné nařízení o ochraně osobních údajů (GDPR) nebo akt o kybernetické odolnosti (Cyber Resilience Act). Slouží-li otázka opatřením z přílohy A normy ISO/IEC 27001:2022, jsou uvedena vedle ní. Na 21 otázek odpovídá každý dodavatel; u každé další je uvedeno, na jaké odpovědi závisí. To se řídí tím, čeho se dodavatel u svých zákazníků dotýká: jejich dat, systémů, prostor nebo softwaru, který provozuje či dodává. Odvětvová rozšíření (TISAX, VDA ISA, německé BSI C5 a KRITIS) tento základ doplňují, nenahrazují.

Zdroj: github.com/NISD2/nis2-supply-chain-questionnaire-schema (MIT + CC BY 4.0)

Licence: MIT (schéma) + CC BY 4.0 (obsah). Volně k použití, převzetí i úpravám.

1. Profil dodavatele

16 polí

Obchodní firma (právní název)

STRING · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2

Zapsaný název vaší společnosti tak, jak je uveden v obchodním rejstříku. Příklad: Novák a syn s.r.o. nebo Příklad Software a.s.

Sídlo společnosti

STRING · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2

Zapsaná obchodní adresa vaší společnosti. Jedna adresa stačí, i když máte více provozoven.

Země

COUNTRY · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2

Země, ve které je vaše společnost právně usazena. Dvě písmena, například CZ pro Českou republiku.

Hlavní doména

DOMAIN · NEPOVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. A)

Vaše hlavní doména, obvykle adresa vašich webových stránek. Příklad: prikladsoftware.cz.

Popis poskytovaných služeb

TEXT · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. B) · ISO/IEC 27001:2022 A.5.19, A.5.22

Jeden odstavec o tom, co zákazníkům dodáváte: konkrétní produkty, služby nebo práce, žádná reklama. Příklady: „Úklid kanceláří tři večery v týdnu, s klíči od budovy“ nebo „Zpracování mezd až pro 200 zaměstnanců“.

Jméno bezpečnostního kontaktu

STRING · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. A) · ISO/IEC 27001:2022 A.5.20, A.5.24

Na koho se zákazníci obrátí, když dojde k bezpečnostnímu incidentu. V menších společnostech často jednatel nebo vedoucí IT. Jedna osoba stačí.

E-mail pro kontakt při incidentech

EMAIL · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. A) · ISO/IEC 27001:2022 A.5.20, A.5.24

E-mailová adresa, kterou zákazníci používají k nahlášení bezpečnostního incidentu. Ideálně distribuční seznam jako bezpecnost@prikladsoftware.cz, který zastihne více osob.

Telefon pro kontakt při incidentech

PHONE · NEPOVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. A) · ISO/IEC 27001:2022 A.5.20, A.5.24

Telefonní číslo pro naléhavá hlášení incidentů. Do závorky uveďte, v jakých hodinách je dostupné; nepřetržitá dostupnost se neočekává.

Jak rychle informujete zákazníky o incidentu (hodiny)

INTEGER · NEPOVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. D) · ISO/IEC 27001:2022 A.5.20, A.5.24

Nejvýše tolik hodin poté, co zjistíte bezpečnostní incident, který se týká zákazníka, například únik dat, napadený účet nebo ztracený klíč. Zákazník, na kterého se vztahuje NIS 2, musí do 24 hodin od okamžiku, kdy se o významném incidentu dozvěděl, podat svému CSIRT nebo úřadu včasné varování (čl. 23 odst. 4 písm. a) NIS 2). Nejvíce mu proto pomůže závazek 24 hodin nebo méně. Uveďte hodnotu, kterou dodržíte.

Poskytujeme SaaS / hostované služby

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. B) · ISO/IEC 27001:2022 A.5.19, A.5.22, A.5.23

Provozujete software pro zákazníky na vlastní infrastruktuře a dodáváte jej přes internet. Pokud nabízíte více modelů, zaškrtněte více políček.

Dodáváme on-premise software

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. B) · ISO/IEC 27001:2022 A.5.19, A.5.22

Dodáváte software, který si zákazníci instalují a provozují na vlastní infrastruktuře.

Poskytujeme spravované služby / MSP

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.2 PÍSM. B) · ISO/IEC 27001:2022 A.5.19, A.5.22

Provozujete pro zákazníka části jeho IT vlastním personálem. Typické pro modely MSP a MSSP.

Zpracováváme nebo uchováváme data našich zákazníků

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1.2 · ISO/IEC 27001:2022 A.5.19

Ano, pokud data nebo dokumenty svých zákazníků uchováváte nebo s nimi pracujete, elektronicky nebo v papírové podobě, například v softwaru, datovém centru, systému pro správu požadavků, účetnictví nebo archivu.

Země / regiony, kde se zpracovávají data zákazníků

STRING · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1.4, TIPY · ISO/IEC 27001:2022 A.5.20, A.5.23, A.5.34

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano

Všechny země, kde se ukládají nebo zpracovávají data vašich zákazníků. Oddělené čárkami, kódy zemí ISO. Příklad: CZ, DE, US. Pokud zpracováváte výhradně v rámci EU, stačí uvést země EU.

Přistupujeme k systémům našich zákazníků

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1.2 · ISO/IEC 27001:2022 A.5.19

Ano, pokud se můžete přihlásit do systémů svých zákazníků, na dálku, jako administrátor nebo na místě, například kvůli údržbě, podpoře nebo provozu.

Naši pracovníci vstupují do prostor našich zákazníků

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 11.1.2 PÍSM. A); BOD 13.3.2 PÍSM. B) · ISO/IEC 27001:2022 A.5.19

Ano, pokud vaši pracovníci nebo subdodavatelé vstupují do kanceláří nebo budov zákazníka, s doprovodem i bez něj, například kvůli úklidu, údržbě, opravám, dodávkám do budovy nebo podpoře na místě. Počítá se i držení klíčů, přístupových karet nebo kódů ke dveřím.

2. Bezpečnostní postupy

31 polí

Pracovníci, kteří pracují pro zákazníky, jsou poučeni o bezpečnosti při nástupu a poté v pravidelných intervalech

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. B) · ISO/IEC 27001:2022 A.6.3

Ano, pokud se všichni, kdo pracují pro zákazníky, seznámí s bezpečnostními pravidly, která pro ně platí, při nástupu a poté znovu v pravidelných intervalech, například na krátkém poučení, v e-learningovém kurzu nebo z písemných pravidel, která podepíší.

Umožňujeme zákazníkům audit nebo jim poskytujeme zprávy z auditu

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. E) · ISO/IEC 27001:2022 A.5.20, A.5.22

Ano, pokud zákazníkům buď umožníte audit, nebo jim místo toho poskytnete zprávy z auditu (například SOC 2, ISAE 3402).

K poskytování služby využíváme subdodavatele

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Ano, pokud se na vaší službě podílejí jiné firmy a dostanou se přitom k datům, systémům nebo prostorám vašich zákazníků. Příklady: poskytovatel cloudu jako AWS nebo Azure, platební služba nebo najatý tým, který pracuje na místě.

Seznam subdodavatelů

TEXT · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Jen pokud: K poskytování služby využíváme subdodavatele = Ano

Všichni subdodavatelé s názvem, místem a tím, co pro vás dělají. Stačí jeden na řádek. Seznam aktualizujte, kdykoli některého přidáte nebo odeberete.

Subdodavatele zavazujeme ke srovnatelným bezpečnostním požadavkům

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. G) · ISO/IEC 27001:2022 A.5.20, A.5.21

Jen pokud: K poskytování služby využíváme subdodavatele = Ano

Ano, pokud vaše smlouvy se subdodavateli obsahují bezpečnostní požadavky, které odpovídají tomu, co po vás požadují vaši zákazníci, například k incidentům, přístupům a zacházení s daty.

Informujeme zákazníky o podstatných změnách, včetně míst, kde se zpracovávají jejich data

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1.4 · ISO/IEC 27001:2022 A.5.22

Ano, pokud zákazníky informujete předem, než se na vaší službě změní něco podstatného: převzetí vaší firmy, nový subdodavatel, jiný poskytovatel hostingu nebo nová země, kde se zpracovávají jejich data.

Na požádání informujeme zákazníky o bezpečnostních incidentech, které zasáhly zákazníky

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1.2 · ISO/IEC 27001:2022 A.5.22

Ano, pokud na dotaz zákazníka otevřeně řeknete, zda a jaké bezpečnostní incidenty s dopadem na zákazníky jste v minulosti měli.

Poskytujeme zákazníkům údaje, které po nich požaduje jejich úřad

BOOLEAN · POVINNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1.4 · ISO/IEC 27001:2022 A.5.20, A.5.31

Ano, pokud svým zákazníkům poskytnete údaje, které po nich jejich dozorový úřad (v Česku NÚKIB) požaduje po incidentu nebo při kontrole. Pokud sami nejste základním nebo důležitým subjektem podle NIS 2 (v Česku poskytovatelem regulované služby podle zákona č. 264/2025 Sb.), nemáte vůči tomuto úřadu přímé povinnosti; povinnost má váš zákazník a vy mu pomáháte ji splnit.

Všichni, kdo pracují pro naše zákazníky, jsou vázáni mlčenlivostí

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1, TIPY; PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 10.3.2 · ISO/IEC 27001:2022 A.6.6

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Naši pracovníci vstupují do prostor našich zákazníků = Ano

Ano, pokud se všichni, kdo pracují pro zákazníky, písemně zavázali k mlčenlivosti, v pracovní smlouvě nebo v samostatné dohodě, nebo je k mlčenlivosti zavazuje zákon.

Ověřujeme, že pracovníci, kteří získají přístup u zákazníků, jsou pro to vhodní

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 10.2.1 · ISO/IEC 27001:2022 A.6.1

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Naši pracovníci vstupují do prostor našich zákazníků = Ano

Ano, pokud před nástupem ověřujete, že lidé, kteří budou mít přístup k datům, systémům nebo prostorám zákazníků (například držitelé klíčů), jsou pro tuto roli vhodní, v rozsahu, který dovoluje pracovní právo a ochrana osobních údajů: například reference nebo, kde je to přípustné a pro roli nutné, výpis z rejstříku trestů. Ověřování všech pracovníků se neočekává.

Na konci smlouvy vrátíme nebo zničíme vše, co od zákazníka máme

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. H); BOD 5.1.2 PÍSM. D) · ISO/IEC 27001:2022 A.5.11, A.8.10

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Naši pracovníci vstupují do prostor našich zákazníků = Ano

Ano, pokud vás smlouva zavazuje vrátit data zákazníka v použitelném, popsaném formátu (například CSV nebo JSON) a poté je smazat, vrátit klíče, přístupové karty a dokumenty a zrušit přístupy, které jste u zákazníka měli.

Smlouva o zpracování osobních údajů (čl. 28 GDPR)

ENUM · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR), ČL. 28 ODST. 3; ČL. 4 BOD 7 · ISO/IEC 27001:2022 A.5.34

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano

Potřebná, pokud zpracováváte osobní údaje jménem zákazníka a podle jeho pokynů (čl. 28 odst. 3 GDPR). Kdo sám určuje účely a prostředky zpracování, je správce a tuto smlouvu jako zpracovatel neuzavírá. Správce může určit i přímo právní předpis (čl. 4 bod 7 GDPR).

- ○ Ano, nabízíme vzorovou smlouvu o zpracování osobních údajů
- ○ Není potřeba: jsme samostatný správce, ne zpracovatel
- ○ Není potřeba: pro zákazníky nezpracováváme žádné osobní údaje
- ○ Ne

Data zákazníků, která uchováváme elektronicky, jsou šifrovaná

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. C); BOD 9.2 PÍSM. A) · ISO/IEC 27001:2022 A.8.24

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano

Ano, pokud jsou data zákazníků šifrovaná všude, kde je elektronicky ukládáte: na serverech, noteboocích, telefonech a v zálohách, například pomocí BitLockeru, FileVaultu nebo šifrování disků u vašeho poskytovatele cloudu.

Data zákazníků, která přenášíme, jsou při přenosu šifrovaná

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. C); BOD 9.2 PÍSM. A) · ISO/IEC 27001:2022 A.8.24

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano

Ano, pokud vaše webové stránky a rozhraní používají HTTPS s TLS 1.2 nebo vyšším a soubory zákazníkům posíláte přes šifrovaný portál nebo šifrovaným e-mailem.

Provozujeme zdokumentovaný systém řízení bezpečnosti informací (ISMS)

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A) · ISO/IEC 27001:2022 A.5.1

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Ano, pokud máte písemnou politiku bezpečnosti informací, jasně přidělené role, pravidelné přezkumy a zdokumentovaný postup při incidentech. Certifikace podle ISO/IEC 27001, i na základě německé metodiky IT-Grundschutz, znamená ano.

Máme platný bezpečnostní certifikát nebo zprávu z auditu, které pokrývají službu, jež dodáváme zákazníkům

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A); ENISA TIG, ODDÍL 5.1.2 · ISO/IEC 27001:2022 A.5.19, A.5.22

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Počítá se: ISO/IEC 27001 (i na základě německé metodiky IT-Grundschutz), atestace podle katalogu C5 německého úřadu BSI, označení TISAX, zpráva SOC 2 Type II nebo ISAE 3402 nebo evropský certifikát kybernetické bezpečnosti. Ano jen tehdy, pokud jeho rozsah pokrývá službu, kterou dodáváte zákazníkům.

Certifikát nebo zpráva: norma, vydavatel, platnost do, rozsah

TEXT · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A); ENISA TIG, ODDÍL 5.1.2 · ISO/IEC 27001:2022 A.5.22

Jen pokud: Máme platný bezpečnostní certifikát nebo zprávu z auditu, které pokrývají službu, jež dodáváme zákazníkům = Ano

Rozsah opište tak, jak je uveden na certifikátu nebo ve zprávě. Máte jich více? Každý na samostatný řádek.

Bezpečnostní aktualizace instalujeme včas a známé zranitelnosti řešíme

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. F) · ISO/IEC 27001:2022 A.8.8

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Ano, pokud máte pro zranitelnosti v systémech a softwaru, které pro zákazníky používáte, pevně stanovený postup: dozvíte se o nich, posoudíte jejich naléhavost a včas nainstalujete aktualizaci nebo přijmete jiné opatření.

Máme písemný plán pro bezpečnostní incidenty

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A); BOD 3.1 · ISO/IEC 27001:2022 A.5.24, A.5.26

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Ano, pokud písemný plán stanoví, jak postupujete při bezpečnostním incidentu: kdo rozhoduje, kdo informuje zákazníky a kdo vše dokumentuje.

Máme písemný plán pro výpadky, včetně záloh

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. C); BOD 4.1; BOD 4.2 · ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.13

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Ano, pokud písemný plán stanoví, jak po výpadku pokračujete v práci nebo znovu spustíte provoz, včetně záloh dat, která pro zákazníky uchováváte, uložených odděleně od provozních systémů a ověřených zkušební obnovou. Plán uvádí vaše kritické systémy, náhradní postup a jak dlouho smí výpadek nejvýše trvat a kolik dat se smí nejvýše ztratit.

Všechny interní administrátorské účty jsou chráněny druhým faktorem

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A); BOD 11.7 · ISO/IEC 27001:2022 A.8.5, A.8.2

Jen pokud: Zpracováváme nebo uchováváme data našich zákazníků = Ano nebo Přistupujeme k systémům našich zákazníků = Ano nebo Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Ano, pokud každý účet s administrátorskými právy ve vašich vlastních systémech (e-mail, cloud, servery, účetnictví) vyžaduje k přihlášení druhý faktor, například ověřovací aplikaci nebo bezpečnostní klíč. Kódy přes SMS se počítají, ale jsou nejslabší možností.

Systémy, kterými obsluhujeme zákazníky, testuje na bezpečnost nezávislá strana

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A); BOD 6.5 · ISO/IEC 27001:2022 A.8.29, A.8.8

Jen pokud: Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano nebo Poskytujeme spravované služby / MSP = Ano

Ano, pokud tyto systémy testuje na zranitelnosti nezávislá strana, tak často, jak to vyžaduje vaše riziko. Počítá se penetrační test i externí sken zranitelností.

Vyvíjíme podle stanovených pravidel bezpečného vývoje

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. A) · ISO/IEC 27001:2022 A.8.25, A.8.28

Jen pokud: Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano

Ano, pokud se váš vývoj řídí pevnými pravidly, například kontrolou každé změny před nasazením do provozu, aktuálními závislostmi, testy a kontrolou známých zranitelností. Ptáme se jen dodavatelů, kteří provozují software jako službu nebo software dodávají.

Zveřejňujeme, jak nám nahlásit zranitelnost

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. F); AKT O KYBERNETICKÉ ODOLNOSTI (CRA), PŘÍLOHA I ČÁST II BODY 5 A 6 · ISO/IEC 27001:2022 A.8.8, A.5.21

Jen pokud: Poskytujeme SaaS / hostované služby = Ano nebo Dodáváme on-premise software = Ano

Ano, pokud na vašem webu stojí, jak vám nahlásit zranitelnost a co pak uděláte, například v souboru security.txt (RFC 9116). Od 11. prosince 2027 vyžaduje akt o kybernetické odolnosti (CRA) od výrobců softwarových produktů takovou politiku a kontaktní adresu.

Do systémů zákazníků přistupujeme přes osobní účty s druhým faktorem

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. A); BOD 11.3.2 PÍSM. A); BOD 11.5.2 PÍSM. B) · ISO/IEC 27001:2022 A.8.2, A.8.5, A.5.16

Jen pokud: Přistupujeme k systémům našich zákazníků = Ano

Ano, pokud každý, kdo se přihlašuje do systémů zákazníků, používá vlastní účet s druhým faktorem, i u nástrojů pro vzdálenou správu, jako je TeamViewer; nikdo nesdílí přihlašovací údaje s ostatními.

Administrátorské přístupy do systémů zákazníků se zaznamenávají

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. A); BOD 3.2.3 PÍSM. E) · ISO/IEC 27001:2022 A.8.15

Jen pokud: Přistupujeme k systémům našich zákazníků = Ano

Ano, pokud se zaznamenává, kdo a kdy přistupoval do systémů vašich zákazníků s administrátorskými právy, aby to šlo později dohledat. Nahrávání celých relací se neočekává.

Evidujeme klíče, přístupové karty a kódy, které nám zákazníci svěřili

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. A); BOD 11.2.2 PÍSM. D); BOD 13.3.2 PÍSM. B) · ISO/IEC 27001:2022 A.7.2, A.5.11, A.5.18

Jen pokud: Naši pracovníci vstupují do prostor našich zákazníků = Ano

Ano, pokud vždy víte, kdo má jaký klíč, kartu nebo kód, odeberete je, když někdo odchází nebo mění práci, a zákazníka bez zbytečného odkladu informujete, když se některý ztratí.

Naši pracovníci se v prostorách zákazníků řídí písemnými pravidly chování

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1, TIPY; PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 8.1.1 · ISO/IEC 27001:2022 A.7.2, A.7.7, A.6.3

Jen pokud: Naši pracovníci vstupují do prostor našich zákazníků = Ano

Ano, pokud mají vaši pracovníci písemná pravidla pro práci u zákazníků, například: nikoho nepouštět dovnitř, nesahat na obrazovky, zařízení a dokumenty, cokoli neobvyklého hlásit zákazníkovi.

Osobní údaje zákazníků mimo Evropský hospodářský prostor

ENUM · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR), ČL. 44; ČL. 45; ČL. 46 ODST. 2 PÍSM. C); ČL. 47

Jen pokud: Smlouva o zpracování osobních údajů (čl. 28 GDPR) = Ano, nabízíme vzorovou smlouvu o zpracování osobních údajů nebo Smlouva o zpracování osobních údajů (čl. 28 GDPR) = Ne

Zda vy nebo vaši další zpracovatelé předáváte osobní údaje zákazníků do země mimo EHP, a na jakém základě. Předání potřebuje jeden ze základů podle kapitoly V GDPR (čl. 44).

- ○ Ne, zůstávají v EHP
- ○ Ano, pouze do zemí, pro které Evropská komise přijala rozhodnutí o odpovídající ochraně (čl. 45)
- ○ Ano, na základě standardních doložek o ochraně osobních údajů přijatých Evropskou komisí (čl. 46 odst. 2 písm. c))
- ○ Ano, na základě závazných podnikových pravidel (čl. 47)
- ○ Ano, na jiném základě

Jak zapojujete další zpracovatele

ENUM · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR), ČL. 28 ODST. 2

Jen pokud: Smlouva o zpracování osobních údajů (čl. 28 GDPR) = Ano, nabízíme vzorovou smlouvu o zpracování osobních údajů nebo Smlouva o zpracování osobních údajů (čl. 28 GDPR) = Ne

Zpracovatel zapojí dalšího zpracovatele jen s předchozím konkrétním nebo obecným písemným povolením zákazníka. U obecného povolení zákazníka informuje o každém zamýšleném přijetí nebo nahrazení, aby mohl vznést námitku (čl. 28 odst. 2 GDPR).

- ○ Obecné povolení: před přijetím nebo nahrazením dalšího zpracovatele vás informujeme a můžete vznést námitku
- ○ Pro každého si vyžádáme vaše konkrétní povolení
- ○ Pro osobní údaje zákazníků nezapojujeme žádné další zpracovatele

Porušení zabezpečení osobních údajů vám ohlásíme bez zbytečného odkladu poté, co se o něm dozvíme

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: OBECNÉ NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR), ČL. 33 ODST. 2

Jen pokud: Smlouva o zpracování osobních údajů (čl. 28 GDPR) = Ano, nabízíme vzorovou smlouvu o zpracování osobních údajů nebo Smlouva o zpracování osobních údajů (čl. 28 GDPR) = Ne

To zpracovatel dluží správci (čl. 33 odst. 2 GDPR). Správce ohlášení potřebuje, aby splnil vlastní povinnost ohlásit porušení dozorovému úřadu (čl. 33 odst. 1).

3. Software jako služba (SaaS)

2 pole

Zákazníci si mohou chránit své účty druhým faktorem

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.2 PÍSM. C); BOD 11.7 · ISO/IEC 27001:2022 A.8.5, A.5.23

Jen pokud: Poskytujeme SaaS / hostované služby = Ano

Ano, pokud vaše aplikace nabízí přihlášení s druhým faktorem (ověřovací aplikace, bezpečnostní klíč nebo jednorázový kód), alespoň pro administrátory vašich zákazníků. Na vaše vlastní interní administrátorské účty se ptá samostatná otázka v části o bezpečnostní praxi.

Nejdelší výpadek do obnovení služby (hodiny)

INTEGER · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: ENISA TIG, ODDÍL 5.1, TIPY · ISO/IEC 27001:2022 A.5.30, A.5.23

Jen pokud: Poskytujeme SaaS / hostované služby = Ano

Nejvyšší počet hodin, po který smí být vaše služba nedostupná, než ji obnovíte. Uveďte hodnotu, kterou dodržíte.

4. Software u zákazníka (on-premise)

4 pole

Do kdy dodáváte bezpečnostní aktualizace pro dodanou verzi

STRING · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 6.1.2 PÍSM. B); AKT O KYBERNETICKÉ ODOLNOSTI (CRA), ČL. 13 ODST. 19 · ISO/IEC 27001:2022 A.5.21

Jen pokud: Dodáváme on-premise software = Ano

Měsíc a rok, nebo pravidlo, podle kterého postupujete. Od 11. prosince 2027 vyžaduje akt o kybernetické odolnosti (CRA), aby výrobci toto datum uvedli při nákupu.

Lhůta pro bezpečnostní aktualizace u kritických zranitelností (hodiny)

INTEGER · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 5.1.4 PÍSM. F); AKT O KYBERNETICKÉ ODOLNOSTI (CRA), PŘÍLOHA I ČÁST II BOD 2 · ISO/IEC 27001:2022 A.8.8

Jen pokud: Dodáváme on-premise software = Ano

Počet hodin od chvíle, kdy se kritická zranitelnost stane známou, do vydání vaší opravené verze. Od 11. prosince 2027 vyžaduje akt o kybernetické odolnosti (CRA), aby výrobci zranitelnosti odstraňovali bez zbytečného odkladu.

Zákazníci mohou dostat soupis softwarových komponent (SBOM)

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 6.1.2 PÍSM. C); AKT O KYBERNETICKÉ ODOLNOSTI (CRA), PŘÍLOHA I ČÁST II BOD 1 · ISO/IEC 27001:2022 A.5.21

Jen pokud: Dodáváme on-premise software = Ano

Ano, pokud zákazníkům ke svým verzím poskytujete SBOM (CycloneDX nebo SPDX). Od 11. prosince 2027 vyžaduje akt o kybernetické odolnosti (CRA), aby výrobci měli SBOM v technické dokumentaci produktů s digitálními prvky; zda ho předáte zákazníkům, je na vás.

Verze a aktualizace jsou podepsané

BOOLEAN · PODMÍNĚNÉ · PRÁVNÍ ZÁKLAD: PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690, PŘÍLOHA, BOD 6.6.1 PÍSM. C); AKT O KYBERNETICKÉ ODOLNOSTI (CRA), PŘÍLOHA I ČÁST II BOD 7 · ISO/IEC 27001:2022 A.5.21

Jen pokud: Dodáváme on-premise software = Ano

Ano, pokud každá verze a každá aktualizace nese podpis, který si zákazníci mohou před instalací ověřit, například Sigstore, Authenticode nebo PGP.