

Kodex informační bezpečnosti pro dodavatele Nestlé



Vydal

Nestlé Information Security

Cílová skupina

Dodavatelé a subdodavatelé Nestlé Česko s.r.o. (dále jen „Nestlé“)

Revidovali

Information Security Manager

LGO Manager

Corporate Affairs Director

Legal Division Director

Procurement Director

Schválil

Generální ředitel Nestlé Česko, s.r.o., leden 2016



Verze

1.0

Autorská práva

Všechna práva naleží Nestlé Česko s. r. o

Úvod ke kodexu informační bezpečnosti pro dodavatele Nestlé

1. Účel

Kodex informační bezpečnosti pro dodavatele Nestlé definuje minimální úroveň informační bezpečnosti, jejíž respektování a dodržování Nestlé vyžaduje od svých dodavatelů a jejich subdodavatelů (dále jen „Dodavatel“).

Tento dokument napomáhá nepřetržité realizaci závazku Nestlé udržovat bezpečné vnitřní a vnější informační prostředí, plynoucího z mezinárodních bezpečnostních standardů, jako jsou například směrnice ISO/IEC 27001 (dále jen „systém řízení bezpečnosti informací“).

2. Rozsah

Kodex informační bezpečnosti specifikuje očekávání kladená na Dodavatele, se kterým Nestlé obchoduje, včetně jeho mateřských, dceřiných nebo přidružených subjektů, včetně všech zaměstnanců (včetně zaměstnanců stálých, dočasných, zaměstnaných přes agenturu a migrujících pracovníků), subdodavatelů a dalších třetích stran, stejně jako na všechny ostatní, se kterými Dodavatel spolupracuje na zpracování dat Nestlé. Dodavatel nese plnou odpovědnost za subdodavatele a další třetí strany, jejichž služeb využívá pro zajištění svých závazků vůči Nestlé, plynoucích pro Dodavatele z tohoto Kodexu. Je zodpovědností Dodavatele rozšiřovat svoji technologickou vyspělost v souvislosti s informační bezpečností, vzdělávat své zaměstnance a svědomitě ověřovat souladu svého prostředí s tímto Kodexem, a to mezi svými zaměstnanci, zástupci a jejich dodavateli na nižším stupni, po-
tažmo všude tam, kde je to relevantní.

3. Soulad

Nestlé očekává, že Dodavatel bude dodržovat všechny platné zákony a předpisy, a to především ty upravující pilíře zde popsané, a bude usilovat o soulad s mezinárodními bezpečnostními standardy a nejlepšími postupy. Dále v souladu s řízením dodavatelů v rámci systému řízení bezpečnosti informací a v souladu s Nestlé Kodexem dodavatele, si Nestlé vyhrazuje právo ověřit soulad jednání a postupů Dodavatele s Kodexem informační bezpečnosti a podmínek vyplývajících z konkrétních smluvních vztahů mezi Nestlé a Dodavatelem, a to prostřednictvím interních nebo externích hodnotících a auditních mechanismů a vyžadovat zavádění změn plynoucích z požadavků auditu nebo požadavků doplňujících systém řízení bezpečnosti informací Nestlé. Dodavatel má povinnost zjištěné nedostatky na své náklady odstranit

4. Nepřetržité zlepšování

Nestlé si uvědomuje, že dosažení standardů stanovených v tomto Kodexu je dynamický proces, a povzbuzuje Dodavatele, aby nepřetržitě vylepšoval své procesy a provozy. V případě, že bude vyžadováno zlepšení, Nestlé poskytne podporu, aby bylo zajištěno zvyšování vzájemné informační bezpečnosti.

5. Použití

Přijetí Kodexu informační bezpečnosti, je stejně, jako přijetí Kodexu dodavatele nutným předpokladem uzavření každé dodavatelské smlouvy s Nestlé. Přijetím objednávky s odkazem na Kodex informační bezpečnosti, se Dodavatel zavazuje, že všechny jeho procesy a provozy jsou v souladu s opatřeními obsaženými v tomto Kodexu.

Pilíře Kodexu informační bezpečnosti, jsou doplňkem a nikoli náhradou bezpečnostních opatření obsažených v rámci jakékoli právní dohody nebo smlouvy mezi Dodavatelem a Nestlé.

Pilíře Kodexu informační bezpečnosti pro dodavatele Nestlé

1. Transparentní informační vztahy

Otevřenost a transparentnost jsou klíčem pro vytvoření pocitu spolehlivosti a důvěryhodnosti při předávání dat mezi obchodními subjekty. Nestlé očekává od Dodavatele, že bude dodržovat základní principy pro zamezení střetu zájmů a vymezí se proti korupčnímu jednání v souvislosti s Nestlé.

Dodavatel v žádném případě netoleruje korupční jednání. Zasaduje se o to, aby jeho zaměstnanci, subdodavatelé, případně zástupci nepřijímali ani nenabízeli či neposkytovali úplatky, nedovolené dary nebo jiné nepřípustné platby či další výhody zákazníkům, veřejným činitelům nebo třetím osobám.

Dodavatel má na paměti platné zákony, zejména zákon o ochraně hospodářské soutěže. S konkurencí, dodavateli ani zákazníky neuzavírá dohody, které by byly v rozporu s pravidly hospodářské soutěže, a nezneužívá případného dominantního postavení na trhu. V souvislosti s tímto Kodexem dbá zejména na etické nakládání s daty při jejich elektronické výměně mezi obchodními subjekty.

2. Ochrana dat

Tímto Kodexem se Dodavatel zavazuje nastavit přiměřenou úroveň ochrany využívaných dat vyplývající z povahy těchto dat a účelu, ke kterému tato data slouží.

Dodavatel je schopen chránit veškerá data, která mohou v případě zveřejnění nebo odhalení způsobit Nestlé významné poškození reputace nebo finanční ztrátu.

Dodavatel respektuje důvěrné informace, know-how, provozní a obchodní tajemství Nestlé. Třetím osobám neposkytuje takové informace bez předchozího výslovného písemného souhlasu Nestlé a nešíří je ani jakýmkoliv jiným nedovoleným způsobem.

Ochrana dat je realizována při přenosu přes veřejnou síť i přes neveřejnou síť Dodavatele. Ochrana dat se vztahuje také na Dodavatelova datová úložiště.

Data musí být chráněna proti poškození, neautorizovanému zneužití, a nesmí být narušena dostupnost, důvěrnost a integrita dat. Dodavatel zajistí, aby data byla řádně uchovávána, a v případě žádosti Nestlé poskytnuta Nestlé zpět.

3. Ochrana osobních a citlivých údajů

Nestlé očekává, že Dodavatel bude dodržovat všechny platné zákony a předpisy týkající se ochrany osobních údajů a citlivých údajů. Jedná se o všechny osobní a citlivé údaje, které jsou zpracovávány Dodavatelem v souvislosti se službami poskytovanými Nestlé.

Dodavatel zajistí, že k osobním a citlivým údajům a jinak důvěrným údajům Nestlé mají přístup pouze oprávnění uživatelé a je povinen ověřovat totožnost pověřených osob.

Dodavatel je zajistí, aby osobní údaje a citlivé údaje Nestlé nebyly uchovávány po dobu delší, než je nezbytné pro poskytnutí služeb, pokud není pokračující uchovávání osobních údajů Nestlé vyžadováno ze zákona.

Na vyžádání je Dodavatel schopen poskytnout Nestlé potvrzení o zničení osobních nebo citlivých údajů.

4. Schopnost reakce

Dodavatel má zavedené mechanismy pro detekci informačních bezpečnostních událostí a incidentů týkajících se dat Nestlé. Tyto události a incidenty je schopen pro snížení možného celkového dopadu nahlásit Nestlé co nejdříve.

Dodavatel se zavazuje nevydávat žádné tiskové prohlášení nebo veřejné oznámení, které souvisí s dokonaným nebo nedokonaným incidentem nebo událostí zahrnující jakákoliv data Nestlé, resp. informace související s Nestlé, bez získání souhlasu Nestlé, není-li to výslovný požadavek zákona nebo jiného právního předpisu.

Nahlášení porušení

Dodavatel nahlásí jakákoliv podezření na porušení předpisů, zákonů a Kodexu informační bezpečnosti pro dodavatele. Porušení by měla být nahlášena kontaktní osobě Nestlé nebo mohou být důvěrně nahlášena s použitím jednoho z dostupných kanálů:

Emailová adresa pro případ podezření na informační bezpečnostní událost nebo incident:

information_security@cz.nestle.com.

Horká linka pro případ velmi závažných informačních bezpečnostních incidentů:

+41 21 924 22 22.

Prohlášení

Potvrzení Dodavatele (Je-li vyžadováno divizí nákupu Nestlé)

My, níže podepsaní, tímto potvrzujeme, že:

- jsme obdrželi a náležitě vzali na vědomí obsah Kodexu informační bezpečnosti pro dodavatele Nestlé z roku 2016, publikovaného společností Nestlé Česko s.r.o.,
- jsme si vědomi všech relevantních zákonů a předpisů v zemích, kde naše společnost působí a společnosti Nestlé Česko s.r.o.,
- nahlásíme jakýkoli případ podezření na porušení Kodexu informační bezpečnosti pro dodavatele Nestlé,
- budeme dodržovat požadavky Kodexu informační bezpečnosti pro dodavatele Nestlé,
- budeme informovat všechny naše zaměstnance / subdodavatele o obsahu Kodexu informační bezpečnosti pro dodavatele Nestlé a zajistíme, aby i oni respektovali s opatření zde uvedená,
- tímto opravňujeme společnost Nestlé Česko s.r.o. nebo jakoukoli organizaci jednající jménem Nestlé Česko s.r.o. kdykoli provádět oznámené i neoznámené audity v našich prostorách, včetně auditů poskytovaných služeb, za účelem ověření souladu s obsahem Kodexu informační bezpečnosti pro dodavatele Nestlé,
- jsme si vědomi, že nebudeme-li dodržovat základní zásady vyplývající z tohoto Kodexu informační bezpečnosti pro dodavatele Nestlé, vyhrazuje si Nestlé právo učinit odpovídající právní kroky a zvážit další spolupráci s námi.

Název společnosti

Podpis / Razítko

Jméno a funkce

Zápis společnosti do obchodního rejstříku/Statutární identifikace/Kód/Číslo

Datum a místo

Tento dokument musí být podepsán oprávněným zástupcem dodavatele a vrácen divizi nákupu Nestlé.

