ZÁVAZEK SPOLEČNOSTI CANON K OCHRANĚ OSOBNÍCH ÚDAJŮ: TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ (TOMS)

OCHRANA ÚDAJŮ A SOUKROMÍ

Canon

Tato technická a organizační opatření pomáhají zajistit, aby společnost Canon plnila povinnosti v oblasti ochrany údajů.

ORGANIZAČNÍ OPATŘENÍ

ZÁSADY

Rámec odpovědnosti společnosti Canon za ochranu osobních údajů se skládá z řady prohlášení o zásadách, která odrážejí různé aspekty ochrany údajů a dodržování předpisů v oblasti ochrany soukromí.

ŘÍZENÍ

K zavedení rámce odpovědnosti v celé oblasti EMEA je využívána komplexní řídicí struktura sestávající ze sítě pověřenců pro ochranu osobních údajů a mistrů ochrany osobních údajů s jasně definovanými rolemi a odpovědností.

ŘÍZENÍ RIZIK

Ke zmírnění rizik v oblasti osobních údajů se používá řada přístupů k řízení rizik, včetně posouzení vlivu na ochranu soukromí, posouzení vlivu na ochranu osobních údajů, dotazníků týkajících se technických a organizačních opatření a komplexních postupů prověrky prodejce.

DŮVĚRNOST

Přístup k údajům zákazníků je povolen pouze v rozsahu nezbytném pro příslušné účely zpracování údajů a na všechny zaměstnance, kteří mají přístup k údajům zákazníků, se vztahuje povinnost mlčenlivosti.

OSVĚTA A POVĚDOMÍ

Osvěta a povědomí posilují rámec odpovědnosti a všichni zaměstnanci, kteří mají přístup ke zpracování osobních údajů nebo jsou za ně odpovědní, musí absolvovat příslušné školení prostřednictvím Centra pro rozvoj společnosti Canon.

PROVĚRKA PRODEJCE

Společnosti třetích stran procházejí prověrkou a údaje zákazníků zpracovávají pouze v souladu se smluvními ujednáními.

ZÁVAZEK SPOLEČNOSTI CANON K OCHRANĚ OSOBNÍCH ÚDAJŮ: TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ (TOMS)

OCHRANA ÚDAJŮ A SOUKROMÍ

ORGANIZAČNÍ OPATŘENÍ (POKRAČ.)

PÉČE O ÚDAJE

Společnost Canon se zavázala k bezpečnému nakládání s osobními údaji, které zpracovává jménem svých zákazníků, a úzce spolupracuje se svými partnery, aby pomohla zajistit dodržování předpisů o ochraně osobních údajů.

PŘEDÁVÁNÍ ÚDAJŮ

Společnost Canon nepředává osobní údaje mimo určitou jurisdikci bez příslušných ochranných opatření, například standardních smluvních doložek v případě EHP.

OZNÁMENÍ A TRANSPARENTNOST

Oznámení společnosti Canon o ochraně osobních údajů odrážejí způsob, jakým skupina spravuje osobní údaje. Při zpracování osobních údajů jsou ústředními zásadami transparentnost a důvěra.

ZÁMĚRNÁ OCHRANA

Ochrana osobních údajů je součástí všech produktů, řešení a služeb v průběhu celého životního cyklu údajů.

PRAVIDLA CHOVÁNÍ

Společnost Canon dodržuje pravidla chování skupiny, která stanoví, že vedoucí pracovníci a zaměstnanci skupiny musí striktně spravovat všechny formy osobních údajů a dodržovat všechny platné zákony a předpisy a předepsané firemní postupy.

ODPOVĚDNOST

Společnost Canon prokazuje odpovědnost tím, že vede komplexní interní záznamy o všech činnostech zpracování osobních údajů, žádostech o práva na informace, porušeních zabezpečení ochrany osobních údajů a postupech posuzování rizik. Naše zákazníky podporujeme také při plnění jejich vlastních povinností týkajících se odpovědnosti.

SPRÁVA NEHOD A KONTINUITA PODNIKÁNÍ

Společnost Canon má zavedeny procesy pro identifikaci, oznámení, řízení, obnovu a řešení případů porušení zabezpečení osobních údajů.

ZÁVAZEK SPOLEČNOSTI CANON K OCHRANĚ OSOBNÍCH ÚDAJŮ: TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ (TOMS)

OCHRANA ÚDAJŮ A SOUKROMÍ

TECHNICKÁ OPATŘENÍ

CERTIFIKACE

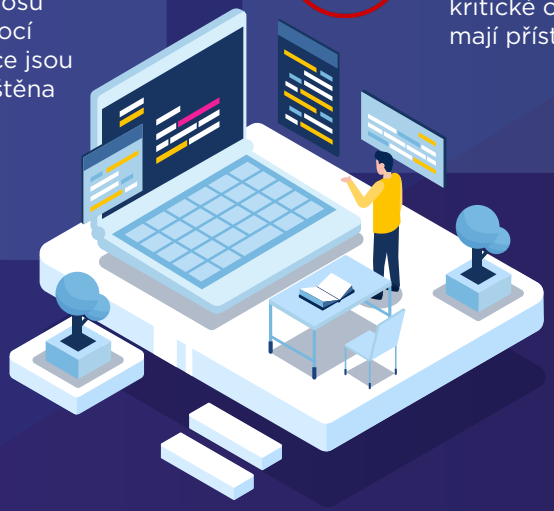
Pokud je to pro daný produkt/řešení/službu vhodné, společnost Canon udržuje příslušné certifikace, například ISO/IEC 27001.

DEIDENTIFIKACE A VÝMAZ

Techniky deidentifikace jsou součástí našich produktů a řešení a mohou zahrnovat anonymizaci a pseudonymizaci a výmaz bez poškození referenční integrity.

ZABEZPEČENÍ DOKUMENTŮ

Společnost Canon chrání osobní údaje při přenosu a v produkčním i neprodukčním prostředí pomocí vhodných kryptografických kontrol. Konfigurace jsou v případě potřeby „posíleny“ tak, aby byla zajištěna bezpečnost zařízení.



ZÁSADY PRO PŘÍSTUP

Zásady a postupy řízení přístupu založené na obchodních požadavcích a požadavcích na bezpečnost informací jsou formálně zdokumentovány, zavedeny a pravidelně revidovány. Tyto zásady a postupy se týkají přístupu oprávněných uživatelů a režimu práce z domova/mobilního pracovních režimu.

KONTROLA PŘÍSTUPU UŽIVATELŮ

Byly zavedeny logické kontroly přístupu. Jedinečné uživatelské účty jsou přidělovány pouze oprávněným osobám a spravovány tak, aby poskytovaly minimální přístup k informacím. Jsou zavedeny kontroly hesel.

FYZICKÉ ZABEZPEČENÍ

Zabezpečené oblasti jsou chráněny vhodnými vstupními kontrolami, které zajišťují, že do oblastí, které obsahují citlivé nebo kritické obchodní informace a zařízení pro zpracování informací, mají přístup pouze oprávnění pracovníci.

ZÁVAZEK SPOLEČNOSTI CANON K OCHRANĚ OSOBNÍCH ÚDAJŮ: TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ (TOMS)

OCHRANA ÚDAJŮ A SOUKROMÍ

Canon

TECHNICKÁ OPATŘENÍ (POKRAČ.)

ODDĚLENÉ PROSTŘEDÍ

Pokud je řešení hostováno, je zajištěno logické oddělení klientů.

VYMĚNITELNÁ MÉDIA

Byly zavedeny kontroly pro správu používání vyměnitelných médií, aby se zabránilo neoprávněnému zpřístupnění, úpravě, odstranění nebo zničení osobních údajů na nich uložených.

BEZPEČNÁ LIKVIDACE NEBO OPĚTOVNÉ POUŽITÍ ZAŘÍZENÍ

Pro všechna média jsou zavedeny postupy bezpečné likvidace a všechny položky zařízení obsahující paměťová média jsou před likvidací nebo opětovným použitím ověřovány, aby bylo zajištěno, že veškeré osobní údaje byly odstraněny nebo bezpečně přepsány podle odpovídajících norem.

PROTOKOL ČINNOSTÍ

Řešení nebo služba může ukládat protokoly činností (například protokol o přístupu uživatelů a správců a o zadávání, změně a výmazu údajů).

MONITOROVÁNÍ

Aktivita uživatelů a systému je monitorována, aby bylo možné identifikovat porušení zabezpečení údajů a zabránit mu.

DOSTUPNOST

Jsou zavedeny kontrolní mechanismy, které zajišťují spolehlivost služeb a nízký výskyt výpadků.

INTEGRACE HARDWARU A SOFTWARU

Dokumentová řešení ve vlastnictví společnosti Canon, jako jsou například uniFLOW a IRIS, nám umožňují rychleji se přizpůsobit novým potřebám zabezpečení a snížit možnost narušení systému.