Belangrijke initiatieven in 2023

Opleidingsprogramma rond de Gedragscode

In 2023 volgde 90% van de bpostgroup-werknemers een opleiding (opgesteld door de afdelingen HR en Compliance) over de Gedragscode. Personeelsleden zonder werk-mailadres volgden een klassikale opleiding. Werknemers met werk-mailadres konden gebruik maken van een specifiek e-learningkanaal. De opleiding bestond uit verschillende onderdelen en benadrukte het belang van verantwoordelijk gedrag in de omgang met klanten en collega's.

Speak Up-programma

In 2023 werd een Speak Up-programma gelanceerd, met een beveiligd kanaal waar mensen 24/7 melding kunnen maken (vertrouwelijk of anoniem). Alle bpostgroup-werknemers werden via brief en e-mail op de hoogte gebracht van de start van het programma, inclusief instructies voor het melden van incidenten. Dezelfde informatie werd ook verspreid via videowanden en posters in alle bedrijfsvestigingen.

4.5 De privacy en veiligheid van gegevens van onze klanten en werknemers waarborgen

Door in alle operationele activiteiten wereldwijd de internationale gegevensbeschermingsnormen volledig toe te passen en in sommige gevallen zelfs te overtreffen, streven we ernaar de veiligheid van werknemers- en stakeholdergegevens te waarborgen.

bpostgroup erkent dat alle informatie, of die nu eigendom is van bpost of in vertrouwen wordt beheerd voor zijn klanten en zakenpartners, en alle ICT-middelen gebruikt om die informatie op te slaan kritieke bedrijfsmiddelen zijn. Daarom verbindt bpostgroup zich ertoe de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen van alle vormen van informatie die gebruikt en bewaard wordt namens zijn personeelsleden, zakenpartners en klanten.

Bijgevolg worden er specifieke policy's, normen, richtlijnen en procedures opgesteld voor de opslag en de verwerking van informatie met het oog op een correcte en wettige bedrijfsvoering. Hierin komen alle informatiebeheeractiviteiten aan bod die een bedreiging of risico vormen voor de lopende activiteiten van bpost, om zo dat risico tot een minimum te beperken of er anderszins toe te komen dat het aanvaardbaar wordt geacht door het toepasselijke managementniveau.

Voorts werd een Roadmap voor Informatieveiligheid ontwikkeld, waarin de stappen en mijlpalen worden beschreven die nodig zijn om het gewenste informatieveiligheidsniveau te bereiken. De Roadmap dient als structuur voor continue verbetering en wordt minstens eenmaal per jaar herzien, om opkomende bedreigingen voor te blijven en erop toe te zien dat de veiligheidsstructuur van bpostgroup nog steeds solide is en het risico op veiligheidslekken miniem.

Een onderdeel van de Roadmap voor Informatieveiligheid is het Bestuursprogramma voor Gegevensbeveiliging, dat verschillende thema's omvat, zoals prioriteiten aanbrengen in gegevens en er inzichten uit puren; goed bestuur en policy's; technieken en beschermingsmaatregelen; en beheer van rechten met betrekking tot informatie. Naast het programma zijn er nog andere initiatieven voor de bescherming van gegevens en gevoelige informatie. Sommige lopen al, andere zijn gepland.

Wat privacy betreft, is de focus gelegd op het reorganiseren van de bestuursstructuren, het verbeteren van het incidentenbeheer en de verdere automatisering van inzageverzoeken van betrokkenen.

Belangrijke initiatieven in 2023

Dataclassificatiepolicy

Als onderdeel van het Bestuursprogramma voor Gegevensbeveiliging is de Dataclassificatiepolicy grondig herzien. Deze policy heeft tot doel alle belanghebbenden een leidraad te bieden en te helpen om de dataclassificatie bij bpost te begrijpen. Bovendien helpt ze gegevenseigenaars, Business Owners, ICT-gegevensbeheerders, onderaannemers en leveranciers te bepalen welk veiligheidsniveau vereist is om de gegevens te beschermen in de systemen van bpost waarvoor ze verantwoordelijk zijn. De classificatie is gebaseerd op het internationaal erkende CIA-schema: Confidentiality – Integrity – Availability (vertrouwelijkheid, integriteit, beschikbaarheid).

Programma voor de opsporing van datalekken

Met de hulp van een externe aanbieder wordt momenteel een programma voor de opsporing van datalekken uitgerold, dat op zoek gaat naar mogelijke lekken van bpostgroup-gerelateerde gegevens en informatie. Het programma bestaat uit:

- Domeinbescherming via monitoring en opsporing van kwaadwillige domeinen die lijken op authentieke bpost-domeinen en zouden kunnen worden gebruikt voor phishingcampagnes en cyberaanvallen
- Monitoring van het darkweb: opsporen en tegengaan van gerichte aanvallen die worden gepland op darkwebfora, in berichtenapps enz.
- Preventie van het overnemen van accounts via monitoring en op zoek gaan naar kritieke lekken van inloggegevens voordat die worden geëxploiteerd
- Preventie van gegevensinbreuken via monitoring, opsporing en veiligstelling van publiek toegankelijke gevoelige gegevens alvorens een inbreuk plaatsvindt

Vragenlijst over informatieveiligheid

Met het oog op naleving van de EU-richtlijn NIS-2 (EU-wetgeving over cyberveiligheid) en meer bepaald van de vereisten inzake de risico's op het vlak van de toeleveringsketen werd een vragenlijst over informatieveiligheid ontwikkeld. Onze leveranciers wordt gevraagd deze in te vullen en waar passend bijkomende veiligheidsmaatregelen in te voeren. Aangezien de vragenlijst gebaseerd is op de ISO 27001-norm voor informatieveiligheid, maakt gegevensveiligheid er integraal deel van uit.

ICT-incidentbeheer

bpostgroup heeft aanzienlijke vooruitgang geboekt in ICT-incidentbeheer, inclusief verbeterde behandeling van gegevensinbreuken. Zo wordt in de Gedragscode de aandacht van bpostgroup-werknemers specifiek gevestigd op incidenten met betrekking tot gegevensinbreuken.