BV Koenraad Vermeulen, Marijke Mellaerts & Valerie Maussen, geassocieerde notarissen

Informatiebeveiligingsbeleid

Version	Date	Changements	Auteur
1.0	2018-03-20	Document initial	Privanot
2.0	2022-12-08	Mises à jour diverses	Privanot
3.0	2023-01-17	Vertaling naar het NL	

Table des matières

1. Inleiding

a. Gegevens van het organisme

Maatschappelijke benaming : BV Koenraad Vermeulen, Marijke Mellaerts & Valerie Maussen, geassocieerde notarissen

Adres: Diestersesteenweg 67, 3583 Paal

Email: marijke.mellaerts@belnot.be

b. Gegevens van de data protection officer

Maatschappelijke benaming : Privanot vzw.

Adres : Bergstraat 30, 1000 Brussel.

Email : info@privanot.be.

a. Doelstellingen van het beleid

Dit beleid verzekert, in overeenstemming met de verplichtingen voorzien in de privacywetgeving of Algemene Verordening Gegevensbescherming (EU) 2016/679 en de andere van kracht zijnde wetten dat de aangewezen technische en organisatorische maatregelen werden ingesteld en functioneel zijn om een passend beveiligingsniveau voor de verwerkte persoonsgegevens te waarborgen, rekening houdend met,

- de aard van de verwerkte persoonsgegevens en de verwerking ervan, alsook met de vereisten inzake vertrouwelijkheid, integriteit en beschikbaarheid;
- de wettelijke of reglementaire vereisten die van toepassing zijn;
- de omvang van het organisme;
- de grootte en complexiteit van de informatiesystemen, informaticasystemen en betrokken applicaties;
- de openheid van het organisme naar buiten toe en de toegangen van buiten uit;
- de risico's waaraan zowel het organisme zelf wordt blootgesteld als de personen van wie de persoonsgegevens worden verwerkt;
- de stand van de techniek ter zake en de kosten die de toepassing van deze maatregelen met zich meebrengt.

Specifiek garandeert dit beleid de bescherming van de gegevens die toegankelijk zijn voor het organisme bij verschillende officiële bronnen.

Meer algemeen laat dit beleid eveneens toe de bescherming te garanderen van de andere persoonsgegevens en de informatie die door het organisme wordt verwerkt.

2. Evaluatie van de risico's

De risico's die de persoonsgegevens lopen, werden geëvalueerd en de maatregelen inzake gegevensbescherming werden daarna vastgelegd in een actieplan.

De verwerkingen van de persoonsgegevens worden gedocumenteerd en hernomen in een specifiek register: het "verwerkingsregister".

3. Classificatie van persoonsgegevens

Vertrouwelijke gegevens

Informatie waarvan de vrije en onbeperkte verspreiding, wijziging, misbruik of oneigenlijk gebruik een aanzienlijke negatieve impact op de organisatie zou hebben, wordt als vertrouwelijk beschouwd. De meeste persoonsgegevens worden van nature als vertrouwelijk beschouwd.

Gegevens voor intern gebruik

Informatie waarvan de vrije en onbeperkte verspreiding, wijziging, verkeerd gebruik of misbruik negatieve gevolgen zou hebben voor de organisatie, wordt als intern beschouwd.

Gegevens vrij van gebruik

Informatie waarvan de vrije en onbeperkte verspreiding geen negatieve gevolgen voor de organisatie zou hebben, wordt als openbaar beschouwd.

4. Informatie voor het personeel

Interne en externe medewerkers betrokken bij dit beleid, werden geïnformeerd over hun verplichtingen inzake vertrouwelijkheid en veiligheid met betrekking tot de verwerkte informatie, die zowel voortvloeien uit de verschillende wettelijke voorschriften als uit het informatiebeveiligingsbeleid.

Interne en externe medewerkers die rechtstreeks betrokken zijn bij de verwerking van informatie worden voldoende geïnformeerd over de verplichtingen inzake beveiliging en gegevensbescherming.

In de van het informatiebeveiligingsbeleid en het arbeidsreglement afgeleide instructies worden de specifieke regels voor de bescherming van informatie en de regels voor het gebruik van informaticamateriaal alsmede de door de werkgever ingestelde controleprocedure gespecificeerd, met name in het kader van het gebruik van e-mail en internet.

5. Identificatie van de dragers

De dragers van persoonsgegevens en de informatiesystemen die deze gegevens verwerken, zijn in geïdentificeerde en beschermde lokalen geplaatst. Enkel de gemachtigde personen hebben toegang tot deze lokalen.

De dragers en informatiesystemen waarop persoonsgegevens staan zijn:

Servers geïnstalleerd in de organisatie ;

Externe servers: NVT

Als principe geldt dat geen enkel gegeven lokaal bewaard wordt en dat geen enkel gegeven op een mobiele drager mag worden opgeslagen (USB-stick, draagbare computer, tablet, enz.), behalve indien dit strikt noodzakelijk blijkt voor de verwezenlijking van de professionele opdracht van de gebruiker die hiervoor van zijn hiërarchisch verantwoordelijke een formele toestemming heeft verkregen. De gegevens worden vernietigd zodra het bewaren ervan niet langer noodzakelijk is voor de verwezenlijking van de nagestreefde opdracht.

6. Fysieke beveiliging van de toegangen

Er werden gepaste beveiligingsmaatregelen ingesteld om onnodige of niet-toegestane fysieke toegangen tot de dragers en informatiesystemen die persoonsgegevens bevatten, te verhinderen.

a. Site A _Diestersesteenweg 67, 3583 Paal

i. Toegang tot de organisatie

De organisatie is open van maandag tot vrijdag, behalve op feestdagen :

De buitendeuren zijn open op:

-maandag en dinsdag van 08:30 tot 18:30;

-woensdag en donderdag van 08:30 tot 18 :00;

-vrijdag van 08:30 tot 12:30

Sluitingsuur: op vrijdag namiddag wordt er gewerkt met gesloten deuren

De medewerkers kunnen steeds met hun eigen sleutel de achterdeur openen en het gebouw betreden. Actief alarm: het alarm is steeds acief in de période dat de laatste persoon het gebouw verlaat en de eerste in de ochtend het gebouw betreed.

ii. Camera's

Er zijn meerder camera's aanwezig, namelijk 1 aan de schuifdeur, de toegang voor de bezoekers, 1 aan de achterdeur, de toegang voor het personeel en zaakvoerders en 1 camera in de onthaal ruimte.

7. Fysieke beveiliging en beveiliging van de omgeving

a. Algemene maatregelen

De nodige beveiligingsmaatregelen werden genomen om fysieke schade die de verwerkte persoonsgegevens in gevaar kan brengen, te verhinderen.

Een brandalarm, rookdetectoren en brandblussers werden in het gebouw van de organisatie geïnstalleerd.

De genomen algemene beveiligingsmaatregelen voor het beschermen van documenten op papier verduidelijken (gesloten ruimtes, niet toegankelijk voor bezoekers, beveiligde kasten enz.).

De genomen algemene beveiligingsmaatregelen voor het beschermen van gevoelige documenten op papier verduidelijken (kluis, brandvrije kast , enz.).

b. Bijzondere maatregelen in de serverruimte van de organisatie

De temperatuur wordt constant gehouden door een airconditioningsysteem. Er is een branddetectie- en beveiligingssysteem geïnstalleerd. Er is een overstromingsdetectiesysteem en/of -pomp geïnstalleerd (deze maatregel geldt alleen voor serverruimten in kelders of op de begane grond). Er is een alternatieve stroomvoorziening geïnstalleerd om de continuïteit van de dienst gedurende een korte periode te waarborgen.

c. Bijzondere maatregelen in de serverruimte van de externe locatie (Niet van toepassing)

De beheerder van de externe locatie neemt ten minste dezelfde of betere maatregelen. Deze is contractueel verplicht om de veiligheidsvoorschriften na te leven.

d. Bijzondere maatregelen voor het Cloud systeem (Niet van toepassing)

De leverancier van het Cloud systeem neemt specifieke gegevensbeschermingsmaatregelen. Deze maatregelen worden aan de leverancier contractueel opgelegd, hetzij rechtstreeks door de organisatie, hetzij door de IT-provider van de organisatie die het Cloud systeem uitbesteedt (indien van toepassing).

In ieder geval worden alle leveranciers van een Cloud systeem steeds duidelijk geïdentificeerd door de organisatie.

8. Netwerkbeveiliging

Het organisme gaat na of de netwerken adequaat beheerd en gecontroleerd worden om ze te beschermen tegen bedreigingen en de bescherming van de systemen en de applicaties die het netwerk gebruiken, efficiënt te waarborgen.

Er is een firewall geïnstalleerd en correct geconfigureerd als computernetwerkbeveiligingssysteem. Alleen de poorten die strikt noodzakelijk zijn voor de goede werking van de organisatie staan open voor de buitenwereld.

Er werd een beveiligde toegang tot het netwerk ingesteld voor het personeel dat toegang tot het netwerk moet hebben (bijvoorbeeld voor telewerken of om een leverancier in staat te stellen onderhoud te plegen). Multifactor authenticatie is hiervoor een vereiste.

Externe verbinding met het netwerk mag alleen plaatsvinden via systemen waarvan de beschermings- en beveiligingsmaatregelen door de organisatie worden gecontroleerd en die ten minste voldoen aan de in dit beleid beschreven vereisten.

9. Beveiliging van servers, werkstations en systemen

Op elke server en elk werkstation is een anti-malwareoplossing geïnstalleerd. De database met malwaredefinities van elke anti-malwareoplossing wordt regelmatig bijgewerkt.

Elk besturingssysteem, software en onderdeel dat is geïnstalleerd op informatiesystemen zoals servers, werkstations, firewalls en andere systemen, wordt regelmatig bijgewerkt met het oog op de veiligheid en wordt nog steeds ondersteund door de fabrikant.

Gebruikerssessies blokkeren of verlopen na een redelijke tijd. Er is anti-malware geïnstalleerd op elke server en werkpost.

10. Beheer van back-ups

Er is een systeem van regelmatige back-ups van alle gegevens noodzakelijk voor de goede werking van de organisatie.

Voor back-ups gelden de volgende maatregelen :

- ten minste één van de back-ups wordt bewaard op een andere locatie dan de serverruimte;
- de gegevens waarvan een back-up wordt gemaakt, worden versleuteld;
- de sleutel voor het decoderen van back-ups is beveiligd in een informatiesysteem op een andere locatie dan de opslaglocatie van de back-ups;
- Back-ups zijn ofwel losgekoppeld van elk netwerk of onveranderlijk (back-ups kunnen niet worden verwijderd van het netwerk van waaruit de back-upgegevens worden verzonden);
- er wordt regelmatig een melding van geslaagde of mislukte back-ups naar de organisatie gestuurd / er wordt real-time monitoring toegepast;
- Back-ups worden regelmatig getest om te herstellen, maximaal 1x per jaar.

11.Vernietiging van gegevens

Papieren documenten met vertrouwelijke of interne informatie worden op een veilige manier vernietigd. Papieren documenten met persoonsgegevens worden vernietigd wanneer de in het "verwerkingsregister" vastgestelde bewaartermijn voor die gegevens is bereikt.

Het vernietigen van vertrouwelijke of interne informatie gebeurd door een erkende vernietingingsfirma, Shred-it. Deze firma komt ter plaatse en vernietigen de documenten "on site".

Persoonsgegevens worden uit de informatiesystemen verwijderd wanneer de bewaartermijn van de gegevens, zoals gedefinieerd in het "Verwerkingsregister ", bereikt werd.

Bij vervanging van IT-apparatuur worden gegevens op media die vertrouwelijke of interne informatie bevatten, veilig vernietigd (vernietiging door de IT-leverancier die een kennisgeving of certificaat van veilige gegevensvernietiging geeft) of worden de media vernietigd op een wijze die de gegevens onbruikbaar maakt (vernietiging van harde schijven met een hamer of boor).

12.Verwerker van persoonsgegevens

Elke verwerker van gegevens is contractueel verplicht om adequate beveiligings- en gegevensbeschermingsmaatregelen na te leven.

13. Logische toegangscontrole

Elke vorm van toegang tot vertrouwelijke of interne informatie gebeurt via een systeem van identificatie, authenticatie en autorisatie van de gebruiker. Autorisaties worden zodanig geconfigureerd dat elke gebruiker alleen toegang heeft tot de vertrouwelijke informatie die hij voor zijn werk nodig heeft, en toegang heeft tot alle interne informatie. De schriftelijke toegang tot openbare informatie verloopt via een soortgelijk systeem.

Persoonsgegevens uit officiële bronnen worden alleen op een veilige manier verzameld via het specifieke portaal.

De toegang tot officiële bronnen en informatiesystemen wordt aangepast naargelang de personeelsveranderingen in de organisatie (indiensttredingen, veranderingen van functies en verantwoordelijkheden, vertrek).

Informatiesystemen die wachtwoordverificatie vereisen, worden centraal geconfigureerd om wachtwoorden te bekomen van ten minste 10 tekens en met een complexe tekeninhoud (hoofdletters en kleine letters, symbolen en cijfers) of een gelijkwaardige of betere bescherming te vereisen. Herhaalde en opeenvolgende vergeefse pogingen om zich op dergelijke systemen te authenticeren hebben tot gevolg dat de gebruikersaccount voor korte tijd wordt geblokkeerd.

De toegang tot informatiesystemen die van buiten de organisatie kunnen worden bereikt (VPN, e-mail, enz.) wordt beschermd door multifactor authenticatie, en verloopt via informatiesystemen die de maatregelen van dit beleid uitvoeren.

Elke gebruiker heeft toegang op naam of is identificeerbaar (generieke of gedeelde accounts zijn niet toegestaan).

Er bestaat een geactualiseerde lijst van de verschillende personen die toegang hebben tot persoonsgegevens uit officiële bronnen. Deze lijst wordt op verzoek aan de gegevensbeschermingsautoriteit ter beschikking gesteld.

14. Toegangsregistratie

De informatiesystemen van de organisatie zijn zodanig ontworpen dat er een logging, spoor en analyse is van de toegang van personen tot informatie en informatiesystemen (directe toegang tot de netwerkstations van de organisatie, toegang via de software van verwerkers, toegang tot het netwerk door een verwerker in het kader van onderhoud, enz.)

Het informatiesysteem van de officiële bron is zodanig ontworpen dat er een logging, spoor en analyse is van de toegang van personen en logische organismen van officiële bronnen.

De volgende elementen worden bewaard :

De identificatiegegevens van de betrokken gebruiker ;

De identificatiegegevens van de persoon op wie de opzoeking betrekking heeft ;

Het moment van de opzoeking ;

Het doel van de opzoeking (informaticatoepassing en/of betreffend dossier).

15. Toezicht, aanpassing en onderhoud

Er wordt voorzien in toezicht op de geldigheid en doeltreffendheid in de tijd van de ingestelde technische of organisatorische maatregelen.

De technische systemen worden getest en onderhouden. Deze zijn contractueel voorzien als er een verwerker of subverwerker bij betrokken is.

Dit beleid en de andere documenten waarnaar wordt verwezen, worden regelmatig herzien.

Het organisme stelt de nodige financiële middelen ter beschikking voor het toezicht, de aanpassing en het onderhoud van de genomen technische en organisatorische maatregelen.

16. Urgentiebeheer van beveiligingsincidenten

Wanneer zich een beveiligingsincident voordoet waarbij verwerkte persoonsgegevens betrokken zijn, wordt de de gedelegeerde voor het dagelijks beheer meteen verwittigd. Deze laatste neemt de nodige maatregelen en kent de bevoegde personen de taken toe om het incident te verhelpen. Op die manier kan het incident gemakkelijk gedetecteerd, opgevolgd en hersteld worden.

Als het incident een datalek is, dan wordt de procedure gevolgd voor de melding van inbreuken op het gebruik van persoonsgegevens.

Handtekening van de gedelegeerde voor het dagelijks beheer:

Dedrij Stephanie
Datum : 25.04.2023
Handtekening