NOTARIAAT WELLENS BV

Informatiebeveiligingsbeleid

Inhoudsopgave

1. Inleiding

a. Gegevens van het organisme

NOTARIAAT WELLENS BV

Eggestraat 28

2640 Mortsel

KBO-nummer: 0874.019.092

DPO : Aurélie Van der Perre, Bergstraat 30-34, 1000 Brussel, 0479/83.18.32, privacy@notaris.be

b. 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 de volgende officiële bronnen:

- Rijksregister;
- Kruispuntbank van de Sociale Zekerheid;
- Kadaster.

Daarnaast verzekert dit beleid de bescherming van de gegevens die toegankelijk zijn voor het organisme bij de volgende officiële bronnen van het notariaat:

- De Centrale Registers van Testamenten en Huwelijkscontracten;
- Het Centraal Register van Lastgevingsovereenkomsten met het oog op het regelen van een buitengerechtelijke bescherming;

- Het Centraal Register van Verklaringen tot aanwijzing van een bewindvoerder of vertrouwenspersoon;

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

Persoonsgegevens die de burger of de medewerkers (loon- en evaluatiesgegevens) betreffen zijn van nature vertrouwelijk. Zij mogen enkel verwerkt worden door personen die gemachtigd zijn om de dossiers van de betrokkenen te beheren, niettegenstaande elk ander wettelijk omkaderd gebruik.

Gegevens voor intern gebruik

Persoonsgegevens die geen burger noch medewerkerkers betreffen of die geen betrekking hebben op tuchtrechtelijke procedures of boekhoudkundige gegevens (voor de kamers) mogen intern gebruikt worden, niettegenstaande elk ander wettelijk omkaderd gebruik.

Gegevens vrij van gebruik

Persoonsgegevens verwerkt door het organisme en voorafgaand geanonimiseerd verliezen hun vertrouwelijk karakter en zijn vrij van gebruik.

4. 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 het kantoor;

Als principe geldt dat geen enkel gegeven lokaal bewaard wordt 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.

Als principe geldt 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.

5. Informeren van het personeel

De interne en externe personeelsleden die betrokken zijn bij dit beleid werden ingelicht over hun plichten ten aanzien van de verwerkte gegevens inzake vertrouwelijkheid en beveiliging die zowel voortvloeien uit de verschillende wettelijke vereisten als uit het beveiligingsbeleid.

Het intern en extern personeel dat rechtstreeks betrokken is bij de verwerkingen van persoonsgegevens is voldoende geïnformeerd over de verplichtingen inzake beveiliging en bescherming van gegevens.

De gedragscode die van toepassing is op het intern en extern personeel en/of het arbeidsreglement leggen de specifieke regels vast die gevolgd moeten worden voor de bescherming van de persoonsgegevens, evenals de regels voor het gebruik van het informaticamateriaal en de controleprocedure die door de werkgever werd ingevoerd, met name in het kader van het e-mail- en internetgebruik.

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.

i. Toegang tot het kantoor

Het kantoor is open van maandag tot vrijdag, behalve op feestdagen:

- De buitendeuren zijn open van 9u tot 12u en van 13u30 tot 18U;
- Kantoren gesloten buiten de normale werkuren.
- Medewerkers bezitten sleutels van het gebouw alsook alarmcode.
- Bezoekers hebben enkel toegang tijdens openingsuren.
- Alarm staat aan buiten normale kantooruren.

ii. Camera's

Er zijn geen camera’s.

7. Fysieke beveiliging en beveiliging van de omgeving

a. Algemene maatregelen

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

Een brandalarm, rookdetectoren en brandblussers werden in het kantoor geïnstalleerd.

Testamenten worden bewaard in een brandveilige koffer.

Akten worden bewaard in een vochtvrije betonnen kelder dewelke niet toegankelijk is voor bezoekers.

Dossiers worden gedigitaliseerd en zijn niet beschikbaar of consulteerbaar voor bezoekers.

b. Bijzondere maatregelen in de serverzaal van het kantoor

De temperatuur blijft constant dankzij het klimaatregelingssysteem. Er werd een systeem geïnstalleerd voor detectie en bescherming tegen brand.

c. Bijzondere maatregelen voor het vernietigen van gegevens

Betreft de vernietiging van gegevens en papieren documenten:

- Dossiers moeten na 30 jaar niet meer bewaard worden;
- De boekhoudingsgegevens na 10 jaar niet meer bewaard worden;
- Akten worden na 75 jaar overgebracht naar het rijksarchief;
- Gegevens en papieren documenten worden op een veilige manier vernietigd door een gespecialiseerd onderaannemer met gdpr-certificaat.

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.

Om schadelijke software te voorkomen en te ontdekken, werden firewall- en antivirussystemen geïnstalleerd; de beveiligingsupdates worden beheerd en geïnstalleerd op de werkposten, servers en apparatuur.

9. Onderaanneming

Elke onderaannemer van persoonsgegevens heeft er zich contractueel toe verbonden de aangewezen maatregelen voor de bescherming en beveiliging van de gegevens na te leven.

10.Lijst met gemachtigde personen

Een geactualiseerde lijst met de verschillende personen die toegang mogen hebben tot de persoonsgegevens van de officiële bronnen kan op verzoek worden opgemaakt.

Deze lijst wordt op verzoek ter beschikking gehouden van de Gegevensbeschermingsautoriteit levenssfeer gehouden.

11.Logische toegangsbeveiliging

De persoonsgegevens zijn enkel toegankelijk via het beveiligde portaal e-Notariaat. De toegang tot de persoonsgegevens gebeurt via een chipkaart met een systeem voor identificatie, authenticatie en machtiging van de gebruiker.

De gebruiksregels van de chipkaart worden verduidelijkt in de gebruiksvoorwaarden van het e-Notariaat.

Het organisme dat verantwoordelijk is voor de toegangen tot het e-Notariaat - de Koninklijke Federatie van het Belgisch Notariaat - wordt onmiddellijk op de hoogte gebracht van het vertrek van een medewerker van het kantoor zodat de toegang zo snel mogelijk kan worden geblokkeerd.

12.Logging van de toegangen

Het informatiesysteem werd zo ontworpen dat logging, opsporing en analyse van de personen en logische entiteiten tot de officiële bronnen mogelijk is. Het systeem wordt opgezet en gewaarborgd door de Koninklijke Federatie van het Belgisch Notariaat.

De volgende gegevens worden bewaard:

- Identificatiegegevens van de betrokken gebruiker;
- Identificatiegegevens van de persoon op wie de opzoeking betrekking heeft;
- Ogenblik van de opzoeking;
- Finaliteit van de opzoeking (informaticatoepassing en/of betrokken dossier).

13.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 onderaannemer 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.

14.Urgentiebeheer van beveiligingsincidenten

Wanneer zich een beveiligingsincident voordoet waarbij verwerkte persoonsgegevens betrokken zijn, wordt de de notaris hiervan 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 ernstige inbreuk is op het gebruik van persoonsgegevens, dan wordt de procedure gevolgd voor de melding van inbreuken op het gebruik van persoonsgegevens.

Een systeem van beveiligingskopieën (back-ups) wordt ingevoerd en wordt regelmatig gecontroleerd om het onherstelbare verlies van gegevens in geval van volledige of gedeeltelijke ramp te vermijden.

Handtekening van de notaris

Paul Wellens
Notaris
1/4/2018