



AVG- EN PRIVACYBELEID

SenS Financiële Diensten

Versie 2.0 – 11 september 2026

Intern beleidsdocument voor de bescherming en zorgvuldige verwerking van persoonsgegevens.

Dit beleid vervangt het AVG-beleid van 1 april 2018. Het beleid wordt ten minste jaarlijks en bij relevante wijzigingen in wetgeving, systemen of bedrijfsvoering beoordeeld.

1. Doel en reikwijdte

SenS Financiële Diensten (hierna: SenS FD) verwerkt in het kader van haar financiële dienstverlening persoonsgegevens van klanten, prospects, contactpersonen en andere betrokkenen. Dit beleid beschrijft hoe SenS FD invulling geeft aan de Algemene verordening gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG) en de privacyverplichtingen die samenhangen met de financiële dienstverlening.

Het beleid geldt voor alle verwerkingen van persoonsgegevens die onder verantwoordelijkheid van SenS FD plaatsvinden, ongeacht of de gegevens digitaal, op papier, per e-mail, via een klantportaal, in een CRM-systeem of op een andere wijze worden verwerkt.

2. Verantwoordelijkheid en privacyorganisatie

SenS FD is voor de eigen bedrijfs- en adviesprocessen in beginsel verwerkingsverantwoordelijke. De verantwoordelijkheid voor naleving van dit beleid ligt bij de leiding van SenS FD. Alleen personen die de gegevens voor hun werkzaamheden nodig hebben, krijgen toegang.

SenS FD is op basis van de huidige aard en omvang van de organisatie niet verplicht een functionaris voor gegevensbescherming (FG) aan te stellen. Deze beoordeling wordt opnieuw uitgevoerd wanneer de organisatie, dienstverlening of gegevensverwerking wezenlijk verandert.

- Vragen, verzoeken van betrokkenen en privacy-incidenten worden centraal beoordeeld en vastgelegd.
- Toegangsrechten worden beperkt tot wat voor de werkzaamheden noodzakelijk is.
- Iedere persoon met toegang tot klantgegevens is gehouden aan geheimhouding.

3. Uitgangspunten van de AVG

SenS FD hanteert bij iedere verwerking de volgende beginselen:

- rechtmatigheid, behoorlijkheid en transparantie;
 - doelbinding: gegevens worden voor vooraf bepaalde en gerechtvaardigde doelen verwerkt;
 - dataminimalisatie: niet meer gegevens verwerken dan noodzakelijk;
 - juistheid: onjuiste gegevens worden waar mogelijk gecorrigeerd;
 - opslagbeperking: gegevens worden niet langer bewaard dan nodig of wettelijk verplicht;
 - integriteit en vertrouwelijkheid: passende technische en organisatorische beveiliging;
 - verantwoordingsplicht: SenS FD kan aantonen hoe aan deze beginselen uitvoering wordt gegeven.
-

4. Doeleinden en rechtsgronden

Persoonsgegevens worden uitsluitend verwerkt wanneer daarvoor een geldige rechtsgrond bestaat. Binnen SenS FD zijn vooral de volgende rechtsgronden relevant:

Doel	Voorbeelden	Voornaamste rechtsgrond
Advies en bemiddeling	Hypotheeken, verzekeringen, kredieten, vermogens- en oudedagsvoorzieningen	Uitvoering overeenkomst / precontractuele maatregelen; waar van toepassing wettelijke verplichting
Wettelijke zorg- en dossierplicht	Inventarisatie klantprofiel, adviesonderbouwing, dossieropbouw	Wettelijke verplichting en uitvoering overeenkomst
Administratie en facturatie	Facturen, betalingen, boekhouding, jaarrekening	Wettelijke verplichting / uitvoering overeenkomst
Klantcontact en service	Afspraken, correspondentie, beheer en nazorg	Uitvoering overeenkomst; in passende gevallen gerechtvaardigd belang
Marketing	Nieuws of aanbiedingen aan relaties/prospects	Toestemming of gerechtvaardigd belang, afhankelijk van kanaal en omstandigheden
Beveiliging en geschilafhandeling	Logging, fraudepreventie, bewijs en behandeling van klachten	Gerechtvaardigd belang en/of wettelijke verplichting

5. Categorieën persoonsgegevens

Afhankelijk van de dienstverlening kan SenS FD onder meer de volgende categorieën verwerken:

- naam, adres, woonplaats, geboortedatum en contactgegevens;
- identificatiegegevens en, uitsluitend waar wettelijk toegestaan en noodzakelijk, het BSN;
- burgerlijke staat, gezinssamenstelling en gegevens over partner of medeverplichtingen;
- inkomens-, vermogens-, pensioen-, uitkerings-, schuld- en betaalgegevens;
- gegevens over woning, onderpand, hypotheek, verzekering of ander financieel product;
- arbeids- en ondernemingsgegevens;
- correspondentie, gespreksnotities, adviesdocumentatie en klantvoorkeuren;
- technische gegevens die noodzakelijk zijn voor beveiliging, logging en toegang tot systemen.

6. Bijzondere persoonsgegevens en BSN

SenS FD streeft ernaar bijzondere persoonsgegevens niet te verwerken, tenzij dit voor een concrete dienstverlening noodzakelijk is én daarvoor een geldige uitzondering op het AVG-verbod bestaat. In de financiële praktijk kan SenS FD bijvoorbeeld incidenteel informatie ontvangen waaruit gezondheidsgegevens blijken, bijvoorbeeld in relatie tot arbeidsongeschiktheid, inkomen of een verzekeringsvraag.

Dergelijke gegevens worden niet breder verwerkt dan noodzakelijk. Medische informatie die uitsluitend voor een verzekeraar of medisch beoordelaar is bestemd, wordt waar mogelijk rechtstreeks via de daarvoor bedoelde beveiligde route verstrekt en niet onnodig in het algemene klantdossier opgenomen.

Het BSN wordt alleen verwerkt wanneer daarvoor een specifieke wettelijke grondslag bestaat. Het BSN wordt niet als algemeen klantnummer gebruikt.

7. Register van verwerkingsactiviteiten

Omdat SenS FD structureel persoonsgegevens verwerkt, houdt SenS FD een register van verwerkingsactiviteiten bij. Het aantal medewerkers is daarbij niet doorslaggevend: structurele, niet-incidentele verwerking maakt een register noodzakelijk.

Het register bevat ten minste de doeleinden, categorieën betrokkenen en persoonsgegevens, categorieën ontvangers, bewaartermijnen en een algemene beschrijving van beveiligingsmaatregelen. Een praktisch register is opgenomen in Bijlage 1.

8. Ontvangers, verwerkers en andere verantwoordelijken

SenS FD deelt persoonsgegevens alleen wanneer dit noodzakelijk is voor de dienstverlening, op verzoek van de klant, op basis van een wettelijke verplichting of op een andere geldige grondslag. Mogelijke ontvangers zijn onder andere geldverstrekkers, banken, verzekeraars, serviceproviders, taxateurs, notarissen, accountants en andere bij de dienstverlening betrokken partijen.

Niet iedere ontvangende partij is een 'verwerker' van SenS FD. Geldverstrekkers, verzekeraars en notarissen zijn voor hun eigen wettelijke en contractuele taken doorgaans zelfstandig verwerkingsverantwoordelijke. Alleen met partijen die persoonsgegevens uitsluitend ten behoeve van en volgens instructies van SenS FD verwerken, wordt waar vereist een verwerkersovereenkomst gesloten.

- SenS FD beoordeelt bij leveranciers welke privacyrol zij hebben.
- Verwerkers worden geselecteerd op voldoende waarborgen voor privacy en beveiliging.
- Afspraken over vertrouwelijkheid, beveiliging, subverwerkers, datalekken en verwijdering/retournering van gegevens worden vastgelegd.

9. Bewaartermijnen en vernietiging

SenS FD bewaart persoonsgegevens niet langer dan noodzakelijk, tenzij een wettelijke bewaarplicht of een aantoonbaar gerechtvaardigd belang een langere bewaartermijn vereist. Het oude uitgangspunt dat een dossier direct na beëindiging van de overeenkomst wordt verwijderd, wordt hiermee vervangen.

Voor adviesdossiers geldt op grond van het Besluit Gedragstoezicht financiële ondernemingen Wft in relevante situaties een minimale bewaartermijn van vijf jaar vanaf het moment van advisering. Voor fiscale basisadministratie geldt in beginsel een bewaarplicht van zeven jaar. Waar andere wettelijke termijnen gelden, worden die gevolgd.

Na afloop van de toepasselijke bewaartermijn worden gegevens verwijderd, geanonimiseerd of op een andere passende wijze buiten gebruik gesteld, tenzij er een concrete reden bestaat om ze langer te bewaren, bijvoorbeeld een lopende klacht, procedure of wettelijke verplichting. Bijlage 2 bevat het bewaartermijnenkader.

10. Technische en organisatorische beveiliging

SenS FD treft, passend bij de aard van de gegevens en de risico's, technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies, onbevoegde toegang, wijziging of verstrekking.

- gebruik van beveiligde systemen en waar beschikbaar multifactorauthenticatie (MFA/2FA);
- unieke accounts en sterke wachtwoorden; bij voorkeur beheer via een betrouwbare wachtwoordmanager;
- beperking van toegangsrechten volgens het need-to-know-principe;
- actuele besturingssystemen, browsers, beveiligingssoftware en beveiligingsupdates;
- apparaatbeveiliging, schermvergrendeling en waar passend versleuteling van gegevensdragers;
- veilige uitwisseling van documenten, bij voorkeur via beveiligde klant- of leveranciersportalen wanneer gevoelige gegevens worden gedeeld;
- periodieke back-ups en herstelmogelijkheden voor bedrijfskritische gegevens;
- zorgvuldige omgang met e-mail, phishing, verdachte links en onverwachte bijlagen;
- veilige vernietiging van papieren en digitale gegevensdragers;
- periodieke controle of gegevens, accounts en toegangsrechten nog nodig zijn.

11. Datalekken en privacy-incidenten

Een datalek is een inbreuk op de beveiliging waarbij persoonsgegevens verloren gaan, worden gewijzigd, vernietigd, ongeoorloofd worden verstrekt of toegankelijk worden voor onbevoegden. Ook een verkeerd geadresseerde e-mail met persoonsgegevens, verlies van een apparaat of onbevoegde toegang tot een account kan een datalek zijn.

Bij een mogelijk datalek wordt de procedure uit Bijlage 3 gevolgd. SenS FD beperkt direct de schade, onderzoekt de aard en omvang, legt het incident vast en beoordeelt of melding aan de Autoriteit Persoonsgegevens (AP) nodig is. Indien een meldplicht bestaat, wordt in beginsel binnen 72 uur na kennisneming gemeld. Bij een hoog risico voor betrokkenen worden ook de betrokkenen onverwijld geïnformeerd, tenzij een wettelijke uitzondering geldt.

Alle datalekken en relevante beveiligingsincidenten worden in een intern datalekregister vastgelegd, ook wanneer geen melding aan de AP nodig is.

12. Privacy by design en privacy by default

Bij nieuwe processen, formulieren, systemen en samenwerkingen beoordeelt SenS FD vooraf welke persoonsgegevens werkelijk nodig zijn en hoe de privacyrisico's kunnen worden beperkt. Standaardinstellingen zijn zo privacyvriendelijk mogelijk.

- Vraag alleen gegevens uit die voor het concrete doel nodig zijn.
- Voorkom onnodige kopieën en dubbele opslag.
- Beperk standaard de toegang tot klantgegevens.
- Beoordeel nieuwe leveranciers en koppelingen vooraf op privacy en beveiliging.

13. DPIA en wijzigingen in verwerking

SenS FD beoordeelt bij nieuwe of wezenlijk gewijzigde verwerkingen of sprake kan zijn van een hoog privacyrisico. Wanneer dat het geval is, wordt vóór de start van de verwerking beoordeeld of een Data Protection Impact Assessment (DPIA) verplicht is en wordt deze zo nodig uitgevoerd.

Aanleidingen voor een nieuwe beoordeling zijn bijvoorbeeld nieuwe technologie, grootschaliger verwerking, koppeling van gegevensbronnen, structurele verwerking van gevoelige gegevens, profilering of geautomatiseerde besluitvorming. De conclusie dat voor de huidige reguliere dienstverlening geen DPIA nodig is, wordt dus niet als permanent gegeven beschouwd.

14. Geautomatiseerde besluitvorming en AI

SenS FD neemt niet uitsluitend op geautomatiseerde verwerking gebaseerde besluiten die voor klanten rechtsgevolgen hebben of hen anderszins in aanmerkelijke mate treffen, tenzij dit rechtmatig is en passende waarborgen zijn getroffen.

Wanneer AI- of andere geautomatiseerde hulpmiddelen worden gebruikt ter ondersteuning van werkzaamheden, blijft SenS FD verantwoordelijk voor een zorgvuldige beoordeling van de uitkomst. Vertrouwelijke klantgegevens worden niet ingevoerd in openbare of niet-goedgekeurde AI-diensten zonder voorafgaande beoordeling van privacy, beveiliging, contractuele voorwaarden en noodzaak.

15. Rechten van betrokkenen

Betrokkenen kunnen, voor zover de AVG dit recht geeft, verzoeken om inzage, rectificatie, verwijdering, beperking van verwerking, overdraagbaarheid van gegevens of bezwaar tegen een verwerking. Ook kunnen zij een verleende toestemming intrekken.

SenS FD controleert bij een verzoek zo nodig de identiteit van de verzoeker en reageert in beginsel binnen één maand. Wanneer de AVG verlenging toestaat, wordt de betrokkene daar tijdig over geïnformeerd. Een verzoek wordt alleen geweigerd of beperkt wanneer daarvoor een wettelijke grond bestaat.

Betrokkenen hebben daarnaast het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

16. Informatieplicht en privacyverklaring

SenS FD verstrekt betrokkenen in duidelijke taal informatie over de verwerking van hun persoonsgegevens, onder andere via de privacyverklaring. De privacyverklaring wordt actueel gehouden en sluit aan op de feitelijke werkwijze.

- identiteit en contactgegevens van SenS FD;
- doeleinden en rechtsgronden van verwerking;
- categorieën ontvangers;
- bewaartermijnen of criteria waarmee deze worden bepaald;
- privacyrechten en de wijze waarop een verzoek kan worden ingediend;
- recht om een klacht bij de AP in te dienen;
- eventuele doorgifte buiten de Europese Economische Ruimte (EER) en de toegepaste waarborgen;
- eventuele geautomatiseerde besluitvorming, indien van toepassing.

17. Doorgifte buiten de EER en cloudleveranciers

SenS FD controleert bij cloud- en IT-leveranciers waar persoonsgegevens worden verwerkt. Indien persoonsgegevens buiten de EER worden doorgegeven, gebeurt dit alleen wanneer daarvoor een geldige doorgiftegrond bestaat en de vereiste waarborgen zijn getroffen. SenS FD vermijdt daarom de absolute verklaring dat gegevens nooit buiten de EU worden verwerkt, tenzij dit aantoonbaar voor alle gebruikte leveranciers en subverwerkers juist is.

18. Geheimhouding, thuiswerken en mobiele apparatuur

Persoonsgegevens worden vertrouwelijk behandeld, ook buiten kantoor. Bij thuiswerken, mobiel werken en gebruik van laptops of telefoons worden dezelfde beveiligingsnormen toegepast als op kantoor.

- Klantdossiers worden niet onbeheerd achtergelaten of zichtbaar gemaakt voor onbevoegden.
- Openbare of onbeveiligde wifi wordt niet gebruikt voor gevoelige werkzaamheden zonder passende beveiliging.
- Verlies of diefstal van een apparaat met toegang tot klantgegevens wordt direct als beveiligingsincident behandeld.
- Privé-opslagmedia en privé-cloudopslag worden niet gebruikt voor klantdossiers tenzij dit expliciet is goedgekeurd en passend beveiligd.

19. Periodieke controle en actualisering

Dit beleid wordt ten minste eenmaal per jaar beoordeeld en daarnaast bij relevante wijzigingen in wet- en regelgeving, dienstverlening, organisatie, systemen, leveranciers of beveiligingsrisico's. Daarbij worden ook het verwerkingsregister, de verwerkersafspraken, bewaartermijnen, toegangsrechten, privacyverklaring en datalekprocedure gecontroleerd.

Versiehistorie:

Versie	Datum	Omschrijving
1.0	01-04-2018	Eerste AVG-beleid SenS Financiële Diensten
2.0	11-09-2026	Volledig geactualiseerd beleid; verwerkingsregister, bewaartermijnen, datalekken, beveiliging, DPIA, ontvangers/verwerkers en AI toegevoegd of aangescherpt

Bijlage 1 – Register van verwerkingsactiviteiten

Onderstaand register is een praktisch basisregister. SenS FD actualiseert het zodra een nieuwe structurele verwerking, leverancier of gegevenscategorie wordt toegevoegd.

Verwerking	Betrokkenen / gegevens	Doel / grondslag	Ontvangers	Bewaartermijn
Hypotheekadvies en -bemiddeling	Klanten/prospects; NAW, contact, ID/BSN waar toegestaan, inkomen, vermogen, schulden, gezin, onderpand, adviesgegevens	Advies, bemiddeling, zorgplicht; overeenkomst / wettelijke verplichting	Geldverstrekkers, serviceproviders, taxateurs, notarissen en overige noodzakelijke partijen	Minimaal wettelijke Wft-termijn; daarna volgens noodzaak en bewaarbeleid
Kredietadvies en -bemiddeling	Klanten/prospects; NAW, contact, ID, inkomen, woonlasten, schulden	Advies/bemiddeling; overeenkomst / wettelijke verplichting	Kredietverstrekkers en noodzakelijke dienstverleners	Volgens toepasselijke Wft- en overige wettelijke termijnen
Levens- en inkomensverzekeringen	Klanten; NAW, contact, financiële gegevens; incidenteel gevoelige gegevens	Advies/bemiddeling; overeenkomst / wettelijke verplichting	Verzekeraars, serviceproviders; medisch beoordelaar waar van toepassing	Volgens toepasselijke Wft-termijn en product-/dossiernoodzaak
Schadeverzekeringen particulier/zakelijk	Klanten; NAW, contact, betaal-, object-, bedrijfs- en risicogegevens	Advies, bemiddeling, beheer; overeenkomst	Verzekeraars, volmacht-/servicekantoren	Volgens wettelijke termijn en duur/noodzaak van relatie
Pensioen/lijfrente/vermogen	Klanten; NAW, contact, ID, inkomen, vermogen, pensioen- en productgegevens	Advies/bemiddeling; overeenkomst / wettelijke verplichting	Banken, verzekeraars, aanbieders, serviceproviders	Volgens toepasselijke wettelijke termijn en dossiernoodzaak
Facturatie en administratie	Klanten/leveranciers; NAW, factuur-, IBAN- en betaalgegevens	Boekhouding, facturatie, fiscale verplichtingen	Boekhouder/accountant, bank, Belastingdienst waar vereist	In beginsel 7 jaar voor fiscale basisadministratie
Website/contactaanvragen	Prospects; naam, contactgegevens, bericht en technische gegevens	Contactverzoek afhandelen; precontractueel / gerechtvaardigd belang	Website-/hosting- of mailleverancier voor zover nodig	Zo kort mogelijk; omzetting naar klantdossier indien relatie ontstaat
Marketing en relatiebeheer	Klanten/prospects; naam, contactgegevens, voorkeuren	Relatiebeheer/marketing	Mail- of CRM-leverancier indien gebruikt	Tot bezwaar/intrekking of zolang passend bij doel en grondslag
Beveiliging en logging	Gebruikers/klanten; account-, toegangs- en loggegevens	Beveiliging, incidentonderzoek, fraudepreventie	IT-/beveiligingsleveranciers voor zover noodzakelijk	Risicobaseerde termijn, niet langer dan noodzakelijk

Bijlage 2 – Bewaartermijnenkader

Bewaartermijnen worden per gegevenssoort bepaald. De langste toepasselijke wettelijke of aantoonbaar noodzakelijke termijn is leidend; gegevens die niet meer nodig zijn, worden eerder verwijderd of geanonimiseerd.

Gegevens / dossier	Uitgangspunt	Toelichting
Adviesgegevens waarop art. 32a BGfo van toepassing is	Ten minste 5 jaar vanaf advisering	Wettelijke minimumtermijn voor de daar bedoelde adviesinformatie en productgegevens.
Fiscale basisadministratie, facturen, grootboek, debiteuren/crediteuren	In beginsel 7 jaar	Fiscale bewaarplicht. Voor bepaalde gegevens kan een langere termijn gelden.
Gegevens over onroerende zaken in de eigen fiscale administratie	Waar van toepassing 10 jaar	Voor btw-gerelateerde gegevens over onroerende zaken kan een langere fiscale termijn gelden.
Niet-geconverteerde prospectgegevens	Zo kort mogelijk	Verwijderen wanneer duidelijk is dat geen relatie ontstaat en geen andere grondslag/noodzaak resteert.
Marketinggegevens	Tot bezwaar/intrekking of einde gerechtvaardigde noodzaak	Suppression/bezwaargegevens mogen beperkt worden bewaard om een bezwaar te respecteren.
Datalekregister	Zolang noodzakelijk voor verantwoordingsplicht en opvolging	Periodiek beoordelen; geen onnodige detailgegevens bewaren.
Klachten/geschillen	Tot einde geschil plus toepasselijke wettelijke/verjaringstermijn	Alleen gegevens bewaren die voor behandeling en bewijs noodzakelijk zijn.
Back-ups	Volgens vast rotatie- en herstelbeleid	Verwijderde gegevens kunnen tijdelijk in back-ups blijven totdat de back-up volgens schema wordt overschreven.

Bijlage 3 – Procedure datalekken en privacy-incidenten

Deze procedure wordt gevolgd zodra een medewerker of leverancier vermoedt dat persoonsgegevens verloren zijn gegaan, verkeerd zijn verzonden, onbevoegd zijn ingezien of anderszins door een beveiligingsincident zijn geraakt.

1. Direct melden en beperken – Meld het incident direct intern. Stop waar mogelijk de oorzaak, trek verkeerd verzonden toegang in, wijzig wachtwoorden of blokkeer accounts en voorkom verdere verspreiding.

2. Feiten vastleggen – Leg datum/tijd, ontdekking, betrokken systemen, soorten persoonsgegevens, vermoedelijk aantal betrokkenen, oorzaak en reeds genomen maatregelen vast.

3. Risico beoordelen – Beoordeel mogelijke gevolgen zoals identiteitsfraude, financieel nadeel, reputatieschade, discriminatie, verlies van vertrouwelijkheid of andere materiële/immateriële schade.

4. Beslissen over melding aan AP – Beoordeel of het datalek waarschijnlijk een risico inhoudt voor rechten en vrijheden van personen. Indien meldplichtig: meld zonder onredelijke vertraging en zo mogelijk binnen 72 uur na kennisneming.

5. Betrokkenen informeren – Bij een waarschijnlijk hoog risico worden betrokkenen onverwijld en in duidelijke taal geïnformeerd, tenzij een wettelijke uitzondering van toepassing is.

6. Registreren – Registreer ieder datalek, ook een niet-meldingsplichtig datalek, inclusief feiten, gevolgen, afweging, besluit en corrigerende maatregelen.

7. Evalueren – Bepaal welke technische, organisatorische of procesmatige verbeteringen nodig zijn en controleer of deze daadwerkelijk zijn uitgevoerd.

Praktische beslisregel: bij twijfel wordt de meldplicht direct onderzocht. De 72-uursperiode begint te lopen zodra SenS FD kennis heeft van een datalek; onderzoek wordt daarom niet onnodig uitgesteld.

Bijlage 4 – Jaarlijkse AVG-controle

- Is het register van verwerkingsactiviteiten nog volledig en actueel?
- Kloppen de privacyverklaring en feitelijke werkwijze nog met elkaar?
- Zijn alle leveranciers beoordeeld op hun rol (verwerker of zelfstandig verantwoordelijke)?
- Zijn noodzakelijke verwerkersovereenkomsten aanwezig en actueel?
- Zijn toegangsrechten, accounts en MFA-instellingen gecontroleerd?
- Zijn bewaartermijnen toegepast en zijn oude dossiers/gegevens waar nodig verwijderd?
- Zijn datalekken en beveiligingsincidenten geëvalueerd en verbetermaatregelen uitgevoerd?
- Zijn nieuwe systemen, AI-toepassingen, koppelingen of werkprocessen beoordeeld op privacyrisico's en eventuele DPIA-plicht?
- Zijn medewerkers/gebruikers opnieuw gewezen op phishing, veilig delen en geheimhouding?
- Zijn back-ups en herstelmogelijkheden aantoonbaar getest?

Juridische basis en onderhoud

Dit interne beleid is opgesteld op basis van de AVG/UAVG, het Besluit Gedragstoezicht financiële ondernemingen Wft (waaronder de relevante dossierbewaarplicht), actuele voorlichting van de



Autoriteit Persoonsgegevens over verantwoordingsplicht, DPIA en datalekken, en de fiscale bewaarplicht zoals toegelicht door de Belastingdienst.

Let op: dit document is een intern beleidskader en geen vervanging voor juridisch advies bij een concreet incident, bijzondere verwerking of wijziging van wet- en regelgeving.