

Privacy- en Securitybeleid

Team P&S

14 januari 2021 | Versienummer 1.0

Versiebeheer

Versie	Datum	Wijziging	Auteur(s)
0.1	6 augustus 2020	startdocument	Jolanda van Drunen, Avenus
0.999	7 januari 2021	Laatste redactieslag na bespreking in ISPMS iav FG	Ieke Coppens (PO/SO)
1.0	14 januari 2021	Laatste wijziging op verzoek van directeur	Ieke Coppens (PO/SO)

Goedkeuring/vaststelling

Gremium	Datum	Besluit
MT	12 januari 2021	Akkoord, m.u.v. Classificatietabel
Directie	13 januari 2021	Akkoord met toevoeging laatste wijziging

Distributielijst

Versie	Naam	Functie/doel
1.0	Directie en MT-leden	Ter informatie (aankondiging in afdelingsoverleggen vooruitlopend op bijscholingssessies door team P&S)

Voorwoord van de directie

Anno 2021 leven we in een informatiemaatschappij waarin data en informatie voor het overgrote deel uitsluitend digitaal worden uitgewisseld. Zeker in dit 'Coronatijdperk' is iedereen 'online' en iedereen heeft tegenwoordig wel eens gehoord van Big Data, de Big Five, van desinformatie, van 'fake news' en 'deep fakes', van 'robotisering', van algoritmen en Kunstmatige Intelligentie. Dit alles brengt nieuwe kansen met zich mee, en uitdagingen, maar ook bedreigingen, en soms ethische dilemma's.

Ook voor VfPf zijn data en informatie van essentiële waarde: zonder data en informatie kan VfPf niet bestaan. In dit beleidsdocument vind je daarom op hoofdlijnen een beschrijving hoe we bij VfPf omgaan met de beveiliging van data en informatie (Security). De bescherming van persoonsgegevens (Privacy) valt daar ook onder. We korten dit af tot Privacy&Security-beleid (P&S-beleid).

Het P&S-beleid draagt bij aan de continuïteit van de belangrijke opdracht die we gezamenlijk voelen: de onderwijssector ontzorgen en ondersteunen bij het borgen van de kwaliteit en continuïteit van het onderwijs zodat lesgeven centraal kan staan. We willen kwalitatief hoogwaardige dienstverlening bieden en besluiten nemen die bijdragen aan het realiseren van onze organisatiebrede doelstellingen en de (bij)sturing daarop. In de toekomst willen we ons ontwikkelen tot een toonaangevend sectorbreed service- en kenniscentrum. Het P&S-beleid levert een bijdrage aan de kwaliteit van data en informatie waar we mee werken en draagt zo bij aan onze missie en visie. Daarnaast is er ook de juridische verplichting om persoonsgegevens te beschermen. Ik doel dan op de Algemene verordening gegevensbescherming die in 2018 van kracht is geworden.

Niemand zal ontkennen dat hierbij van cruciaal belang is, dat de data waarmee we werken *betrouwbaar* zijn. En dan rijst onmiddellijk de vraag: wanneer zijn data betrouwbaar? Welke kwalitatieve eisen stellen wij als VfPf eigenlijk aan onze data? En om welke soorten data gaat het dan? Aan welke bedreigingen worden die data feitelijk blootgesteld? En hoe groot is het risico dat die data daar ook door wordt getroffen?

In deze digitaal gedomineerde samenleving onttrekken data zich aan onze fysieke waarneming, en dat maakt het nu juist zo lastig, omdat op het eerste oog niet meteen zichtbaar is wat er met die data gebeurt. En juist daar gaat het om: alléén als we weten wat er precies met 'onze' data gebeurt en waardoor die data bedreigd worden, kunnen we de verantwoordelijkheid daarover nemen en de betrouwbaarheid van onze data garanderen.

Alle vragen die ik hierboven heb opgeworpen moeten we dus met elkaar beantwoorden om te komen tot een doeltreffend pakket aan maatregelen om de betrouwbaarheid van onze data te waarborgen. We doen dan wat nodig is om onze belangrijkste data sterk te beveiligen, en onze minder belangrijke data minder sterk te beveiligen. Anders gezegd: we treffen *passende* maatregelen. En periodiek bekijken we, of die maatregelen nog voldoen.

Ik wijs tot slot met nadruk op de concepten *Privacy by Design and Default* en *Security by Design and Default*. Er verandert veel bij VfPf, ook de komende jaren nog. Privacy & Security moeten al vanaf het begin van de ontwikkeling van nieuwe diensten en producten voor onze klanten meegenomen worden. Dit niet alleen omdat de AVG ons dat oplegt, maar vooral omdat onze klanten en stakeholders dat van ons mogen verwachten.

Denis Vijgen,



1	DOELGROEP, DEFINITIE EN DOELSTELLINGEN P&S-BELEID	5
1.1	Doelgroep P&S.....	5
1.2	Definitie P&S in 6 begrippen.....	5
1.3	Doelstellingen P&S-beleid	5
2	AVG EN ISO27001	6
2.1	Passende technische & organisatorische maatregelen	6
2.2	De AVG toegelicht.....	7
2.3	De ISO 27001/2 (2017) toegelicht	8
3	VERANTWOORDELIJKHEDEN P&S	9
3.1	Algemene verantwoordelijkheid medewerkers	9
3.2	Naleving	9
4	SLOTOPMERKINGEN	9
5	REFERENTIEDOCUMENTEN.....	9

1 Doelgroep, definitie en doelstellingen P&S-beleid

1.1 Doelgroep P&S

Dit Privacy- en Securitybeleid is geschreven voor iedereen die voor VfPf werkt. Of je nu in vaste dienst bent of op tijdelijke basis voor VfPf werkt, of werkzaam bent bij één van onze leveranciers: aan Privacy en Security moet iedereen een steentje bijdragen. Privacy & Security raakt álle afdelingen en lagen van VfPf en álle disciplines daarbinnen. Dan kun je denken aan Directie en Management, Informatievoorziening, Informatie- en Communicatietechnologie (ICT), Personeel & Organisatie (PO), Procesmanagement, Control, Risicomanagement en Communicatie. Wat we in eerdere beleidsversies hebben benoemd geldt nog steeds: Privacy & Security is van iedereen en hoort bij ons gewone, dagelijkse werk.

1.2 Definitie P&S in 6 begrippen¹

VfPf gebruikt bij zijn taken allerlei Gegevens, waaronder ook persoonsgegevens. Persoonsgegevens zijn gegevens die ofwel direct over iemand gaan, ofwel (zonder al te veel moeite) naar deze persoon te herleiden zijn. Dat persoonsgegevens moeten worden beschermd zal niemand tegenwoordig meer verbazen: iedereen heeft wel eens gehoord van de Algemene verordening gegevensbescherming (afgekort: AVG). Met de term Privacy doelen we op de bescherming en beveiliging van de persoonsgegevens die VfPf gebruikt.

VfPf gebruikt niet alléén persoonsgegevens. Oók andere informatie dan persoonsgegevens willen we beschermen en beveiligen. Denk aan bedrijfsgevoelige informatie, zoals Jaarplannen en financiële gegevens, en aan technische data, zoals broncodes. Of denk aan informatie, die minder bedrijfsgevoelig is, zoals beleidsdocumenten, procesbeschrijvingen en werkinstructies. Denk ook aan algemene en openbare informatie over onze activiteiten, producten en diensten. Met de term Security doelen we op de beveiliging van álle soorten van informatie die VfPf gebruikt.

Data en Informatie moet betrouwbaar zijn. We drukken de betrouwbaarheid van data/informatie uit in de mate waarin die Beschikbaar, Integer en Vertrouwelijk (BIV) is.

- Beschikbaarheid: data/informatie en systemen/applicaties moeten op de juiste momenten **Beschikbaar** zijn: hebben gebruikers op de juiste momenten toegang tot de data/informatie en systemen/applicaties die ze voor hun werk nodig hebben?
- Integriteit: de data/informatie en systemen/applicaties moeten **Integer** zijn: is waar we mee werken en hoe we dat doen juist, is het volledig?
- Vertrouwelijkheid: de data/informatie en systemen/applicaties moeten **Vertrouwelijk** zijn en blijven waar dat nodig is: hebben alléén personen toegang tot data/informatie

1.3 Doelstellingen P&S-beleid

Dit beleid geeft kaders voor het bereiken van de doelstellingen voor de bescherming en beveiliging van ze data/informatie. AVG en ISO zijn hierin leidend. De beleidsstukken die met dit beleid samenhangen geven hier verdere invulling aan. Vooral de beleidsstukken 'Classificatiebeleid', 'Technisch beleid' en 'Handboek P&S' zijn daarbij van belang: deze documenten geven verdere invulling, verdieping en concretisering aan dit beleid. Gedragsregels voortvloeiend uit dit beleid zijn opgenomen in het Personeelshandboek van VfPf.

¹ Een lijst met de belangrijkste begrippen op het gebied van P&S tref je aan in **Bijlage 1: Begrippenlijst**, bij dit document. Alle onderstreepte hoofdletterwoorden van dit document vind je op die lijst terug. Voor de meest actuele versie van de P&S-begrippenlijst verwijzen we naar G:\Privacy en Security\1. P&S-beleid VfPf, Infographic P&S VfPf en Handleiding AVG.

Doelstelling	Hoe te behalen
VfPf is op zo'n manier georganiseerd dat we onze werkzaamheden om het ISPMS in stand te houden nu én in de toekomst kunnen blijven uitvoeren conform de vereisten van ISPMS	<p>We beleggen onze taken en verantwoordelijkheden binnen de organisatie en leggen werkwijzen en maatregelen vast (Handboek P&S)</p> <p>We treffen organisatorische maatregelen en leggen bewijs vast</p>
VfPf beheerst zijn risico's op het gebied van Privacy & Security (BIV)	<p>We voeren minimaal jaarlijks risicoanalyses uit en leggen bewijs vast</p> <p>We treffen technische maatregelen (reductie van kwetsbaarheden, misbruik van gegevens) en leggen bewijs vast</p>
VfPf voldoet aan beleidsregels, processen en procedures inclusief andere werkafspraken ten aanzien van Privacy & Security	<p>Wij trainen onze medewerkers minimaal jaarlijks op het gebied van bewustzijn en leggen bewijs vast</p> <p>Nieuwe medewerkers krijgen binnen een maand na indiensttreding een passende bewustzijnstraining en we leggen bewijs vast</p> <p>Jaarlijks worden interne audits uitgevoerd om te bepalen of er aan de door de organisatie gestelde eisen wordt voldaan</p> <p>Afwijkingen worden vastgelegd en vormen de basis voor continue verbetering</p>

2 AVG en ISO27001

Bij VfPf wordt P&S vormgegeven door twee belangrijke kaders, te weten:

- de Algemene verordening gegevensbescherming (AVG)
- de BIR/BIO/ISO 27001/2 (uit 2017)

De AVG is de Europese wetgeving op het gebied van Privacy die op VfPf van toepassing is en waar we dus aan moeten voldoen. De ISO 27001/2 is een wereldwijd erkende norm op het gebied van Security. Organisaties kunnen daarvoor certificeren als een onafhankelijke auditor heeft vastgesteld dat voldaan is aan deze internationale norm.

Zowel op grond van de AVG als op grond van de ISO 27001/2 moet VfPf "*passende technische en organisatorische maatregelen*" nemen om (persoons-)gegevens/data/informatie te beschermen. De vraag is dus: hoe komt VfPf tot "*passende technische en organisatorische maatregelen*"? Het antwoord op die vraag is: door dataclassificatie en door risicoanalyses. Dataclassificering en risicoanalyses geven antwoord op de vraag hoe scherp de set aan technische en organisatorische maatregelen moet zijn om ervoor te zorgen dat onze data/informatie betrouwbaar is en ook blijft. Het beleid van VfPf op dit punt is te vinden in dit document, het Dataclassificatiebeleid en het Technisch beleid van VfPf. De (processen rondom) risicoanalyses P&S zijn beschreven in het Handboek P&S.

2.1 Passende technische & organisatorische maatregelen

Dataclassificatie begint bij het aanmaken van Informatiegroepen. Dat zijn soorten informatie die een bepaalde mate van vertrouwelijkheid gemeen hebben. Bij VfPf onderscheiden we er 4: openbare, interne, bedrijfsvertrouwelijke en vertrouwelijke informatie. Deze 4 Informatiegroepen zijn omschreven in onderstaande tabel. De blauwe kolom maakt in één oogopslag duidelijk hoe vertrouwelijk we die data/informatie vinden en aan wie we die data/informatie dus kunnen/mogen verstrekken.

Omschrijving Informatiegroep	Wettelijke eisen	Classificatie Vertrouwelijkheid	Resultaat: Classificatie Informatiegroep
Algemene informatie, publiekelijk beschikbaar, over activiteiten, producten en diensten van VfPf, zoals folders, leaflets, flyers, presentaties, rapportages en onderzoeken, bestuursbesluiten op de website VfPf, etc.	Geen	Openbaar: Informatie is publiekelijk beschikbaar en mag vrijelijk verstrekt worden	Classificatieniveau-0
Operationeel beleid, processen, procedures, plannen, rollen etc.	Geen	Intern gebruik: Informatie is beschikbaar voor alle interne medewerkers en door het management geselecteerde derde partijen. Deze informatie mag alleen aan interne medewerkers en door het management geselecteerde derde partijen verstrekt worden	Classificatiegroep-1
(Commercieel) vertrouwelijke stukken, zoals offertes, prijsopgaves, contracten, facturen en andere documenten met commercieel vertrouwelijke informatie. Verder bedrijfsinformatie over derde partijen (kengetallen, solvabiliteit e.d.) waarover VfPf beschikt, bv. in het kader van due diligence, etc. Verder ook de uitkomsten/rapportages over bv. penstesten in het kader van P&S	Wet toezicht financiële verslaglegging (Wtffv), Aanbestedingswet 2012	Bedrijfsvertrouwelijk: Informatie is alleen beschikbaar voor geautoriseerde personen. De informatie mag alleen aan geautoriseerde personen verstrekt worden, niet aan derde partijen	Classificatiegroep-2
(Persoons)gegevens van klanten, consumenten, werknemers en Bestuursleden, AC-leden etc., technische gegevens, configuraties, broncode, etc.	Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG)	Vertrouwelijk: Informatie is alleen beschikbaar voor geautoriseerde personen. De informatie mag alleen aan geautoriseerde personen verstrekt worden, niet aan derde partijen	Classificatiegroep-3

Het Technisch beleid van VfPf beschrijft de basisset aan maatregelen die gelden voor deze data/informatie in onze systemen/applicaties. Als de BIV-dataclassificatie van data/informatie in (de context van) onze systemen/applicaties een hogere BIV-score opleveren, stappen we over naar een scherpere set technische maatregelen. Zo kunnen we een hoger beschermingsniveau garanderen. Afhankelijk van specifieke risico's die we in risico-analyses zien, passen we de totale set technische en organisatorische maatregelen nóg verder aan.

2.2 De AVG toegelicht

De AVG beschijft niet concreet wat wél en wat niet mag met persoonsgegevens, maar geeft een aantal beginselen bij het gebruik ervan. In een notendop kunnen die beginselen als volgt worden samengevat.

1. VfPf maakt alleen gebruik van persoonsgegevens als daar een juridische basis voor is. In de AVG heet dat **Gerechtvaardigde grondslag**. Als we gebruik maken van persoonsgegevens zorgen we ervoor dat de personen over wie het gaat over dat gebruik zijn ingelicht. Dit doen we door een zogenaamde **Privacyverklaring** op te stellen en te publiceren. Zo'n verklaring wordt ook wel het Privacy Statement genoemd. Het spreekt voor zich dat een Privacyverklaring actueel moet worden gehouden.
2. Als VfPf gebruik maakt van persoonsgegevens zorgen we ervoor dat we hebben beschreven waarom/waarvoor we die persoonsgegevens gebruiken (het zogenaamde "doeleinde"). Willen we die persoonsgegevens voor een ánder doel gaan gebruiken, dan is dat alleen toegestaan als dat andere doel inhoudelijk samenhangt met het doel waarvoor de gegevens aanvankelijk werden gebruikt. In de AVG heet dat **Doelbinding** ("niet onverenigbare verdere verwerking").
3. VfPf maakt alléén gebruik van persoonsgegevens die werkelijk nodig zijn voor de uitvoering van ons werk. In de AVG heet dit **Minimale gegevensverwerking**.

4. VfPf maakt gebruik van persoonsgegevens die juist zijn en we actualiseren die persoonsgegevens.
5. VfPf bewaart persoonsgegevens niet langer dan nodig is. Daarom leggen we de Bewaartermijn van persoonsgegevens vast en verwijderen we die persoonsgegevens als die termijn voorbij is.
6. VfPf neemt “**passende technische en organisatorische maatregelen**” om de persoonsgegevens die we gebruiken te beveiligen. Dit betekent dat we kiezen voor een niveau van beveiliging dat past bij de **risico's** die we daarbij inschatten.

Verder brengt de AVG een aantal concrete verplichtingen voor VfPf met zich mee. In een notendop kunnen die verplichtingen als volgt worden samengevat:

1. VfPf moet “**passende technische en organisatorische maatregelen**” nemen om ervoor te zorgen dat de AVG wordt toegepast.
2. VfPf past Privacy by Design toe, vertaald als gegevensbescherming door ontwerp. Dit betekent dat we bijvoorbeeld al bij de aanbesteding van een opdracht rekening houden met eisen op het gebied van P&S. Het betekent bijvoorbeeld ook dat we bij het bouwen van een applicatie al nadenken over eisen op het gebied van P&S. Ook past VfPf Privacy by Default toe, vertaald als gegevensbescherming door standaardinstellingen. Dit betekent dat we al aan de start van innovaties en/of verbeteringen Privacy & Security-beginselen toepassen, en niet pas achteraf.
3. Als VfPf samen met een andere organisatie persoonsgegevens gebruikt, spreken we af welke organisatie welke verantwoordelijkheden draagt.
4. VfPf mag een derde partij opdracht geven de werkzaamheden met persoonsgegevens uit te voeren (uitbesteden). Zo'n partij heet in de AVG: Verwerker. Voorwaarde hiervoor is dat we met Verwerkers een Verwerkersovereenkomst sluiten. De AVG bevat een aantal eisen waar zo'n Verwerkersovereenkomst aan moet voldoen.
5. VfPf houdt een Verwerkingenregister bij. In dat register nemen we per Verwerking van persoonsgegevens minstens de door de AVG voorgeschreven gegevens op.
6. VfPf meldt binnen 72 uur na ontdekking van een datalek dat datalek bij de Autoriteit Persoonsgegevens. Als dit datalek een hoog risico voor betrokkenen inhoudt meldt VfPf dat ook bij die betrokkenen. Zo stellen we betrokkenen in staat om zelf eventuele risico's aan te pakken.
7. VfPf voert een risico-analyse uit bij gebruik van persoonsgegevens dat waarschijnlijk een hoog risico voor betrokkenen oplevert. In de AVG heet dit een Data Protection Impact Assessment. Dit laat zich vertalen tot Gegevensbeschermingseffectbeoordeling, en korten we gemakshalve af tot DPIA. Als daarbij blijkt dat geen maatregelen mogelijk zijn die Privacyrisico's verlagen, schakelen we de Autoriteit Persoonsgegevens (AP) in. De AP brengt dan een advies uit. In de AVG heet dat “Voorafgaande raadpleging”.
8. VfPf stelt een Functionaris voor Gegevensbescherming aan (afgekort tot FG). De belangrijkste taak van de FG is toezien op de naleving van de AVG en het P&S-beleid van VfPf.

2.3 De ISO 27001/2 (2017) toegelicht

De ISO 27001/2 beschrijft in feite de voorwaarden waaraan een zogenaamd Information Security Management System (ISMS) moet voldoen. VfPf heeft dit beschreven in het 'Handboek P&S'. Het ISMS is bij VfPf de motor van de activiteiten op het gebied van P&S en wordt onderhouden middels de plan-do-check-act cyclus. Het doel van een ISMS is continu beoordelen of de beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Een belangrijk uitgangspunt is hierbij dat we denken in termen van risico's en die risico's prioriteren. Daarom brengen we in die risico's een rangorde aan: Hoog, Midden of Laag. Uitgangspunten bij de omgang met deze risico's zijn:

- Als een risico als 'laag' wordt bestempeld dan kiezen we ervoor om dat risico te accepteren, tenzij het niet aanpakken van een laag risico op termijn tot een hoger risico kan leiden.
- Als een risico als 'midden' of 'hoog' wordt bestempeld neemt de risico-eigenaar in overleg met de directie altijd maatregelen, tenzij dat niet mogelijk is en/of de baten niet opwegen tegen de kosten.

3 Verantwoordelijkheden P&S

3.1 Algemene verantwoordelijkheid medewerkers

VfPf verwacht van mensen die voor VfPf werkzaam zijn, dat ze zich bewust zijn van de risico's die er zijn als het gaat om data/informatie. Veilig werken met data/informatie in onze systemen is een verplicht onderdeel van ieders takenpakket.

Om te helpen bij het vergroten van het risicobewustzijn biedt VfPf met geregelde tussenpozen awareness-sessies en trainingen aan op het gebied van P&S. Zo bereiken we dat iedereen zich bewust is van risico's op het gebied van P&S en in staat is veilig om te gaan met data/informatie. In het uiterste geval kunnen zelfs disciplinaire maatregelen worden genomen. Dit is voor interne medewerkers vastgelegd in het Personeelshandboek dat onlosmakelijk onderdeel uitmaakt van ieders arbeidsovereenkomst met VfPf. Als het gaat om externe medewerkers zijn verantwoordelijkheden ten aanzien van P&S vastgelegd in een overeenkomst van opdracht.

Iedereen werkzaam voor VfPf moet Security-incidenten en Datalekken kunnen herkennen en deze zo snel mogelijk per telefoon of e-mail melden bij de Security Officers van VfPf.

3.2 Naleving

Om er zeker van te zijn dat P&S bij VfPf écht werkt, worden alle beveiligingsmaatregelen gecheckt door interne - en externe controles. Met controles kunnen we aantonen, ook aan derden, dat het P&S-beleid gevolgd wordt. Dit betekent onder andere dat:

- *We controleren dat werknemers veilig werken, als onderdeel van het werk;*
- *We periodiek interne en externe controles en audits uitvoeren om het beleid te controleren;*
- *We actie nemen als uit controles en audits afwijkingen naar voren komen.*

4 Slotopmerkingen

De Directie wordt over dit P&S-beleid geadviseerd door team P&S en waar wenselijk door de FG. De Directie stelt het P&S-beleid vast door ondertekening ervan, waarna het in werking treedt. Het management van VfPf is eindverantwoordelijk voor de uitvoering van het P&S-beleid. Team P&S monitort de naleving van het beleid en adviseert de Directie over handhaving. Eens per drie jaar herzien we ons P&S-beleid, of zoveel eerder als daar concreet aanleiding voor is.

De Functionaris Gegevensbescherming (FG) is hierbij op grond van de AVG een onafhankelijke toezichthouder die erop toeziet dat VfPf conform de AVG en het P&S-beleid van VfPf handelt. Verder is de FG contactpersoon in de samenwerking en contacten tussen de Autoriteit Persoonsgegevens (AP) en het VfPf.

5 Referentiedocumenten

- a. Algemene verordening gegevensbescherming (AVG);
- b. Richtsnoeren Security Rijksoverheid (BIR, BIO);
- c. ISO/IEC 27001, normelement 5.2 en 6.2;
- d. Handboek P&S VfPf;
- e. Classificatiebeleid VfPf;
- f. Technisch beleid VfPf.

Bijlage 1: BEGRIPPENLIJST

Applicatie: een computerprogramma dat bedoeld is voor eindgebruikers. Letterlijk vertaald betekent het "toepassing"; vaak ook afgekort als "app".

Bedrijfsmiddelen: informatiesystemen en andere informatie/apparatuur, inclusief papieren documenten, mobiele telefoons, draagbare computers, media voor gegevensopslag, enz.

Beschikbaarheid: kwaliteitseis aan data/informatie en systemen/applicaties die moet verzekeren dat de data/informatie en systemen/applicaties beschikbaar zijn voor bevoegde personen als dat nodig is.

Betrouwbaarheidseisen: eisen die VfPf stelt aan data/informatie en systemen/applicaties op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

Classificaties: groepen van data en/of informatie en systemen/applicaties met gelijksoortige betrouwbaarheidseisen.

Classificeren: indelen in classificaties.

Data: (in een bestand) opgenomen uitdrukkingen van feiten. Zie ook gegevens.

Datalekken: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Gegevens: (in een bestand) opgenomen uitdrukkingen van feiten. Zie ook: data.

Incident: een gebeurtenis met ongewenste gevolgen, bv. een beveiligingsincident.

Informatie: data of gegevens die zijn geïnterpreteerd en geïntegreerd, zodat die informatie kennis oplevert.

Informatiegroepen: groepen van verschillende soorten data/informatie die een bepaalde mate van vertrouwelijkheid gemeen hebben.

Informatiesystemen: alle servers en cliënten, netwerkinfrastructuur, systeem en ondersteuning bij programmeren, gegevens en andere computer subsystemen en onderdelen die eigendom zijn van of worden gebruikt door VfPf of die onder de verantwoordelijkheid van VfPf vallen. Het gebruik van informatiesystemen bevat alle interne en externe diensten, zoals internettoegang, e-mail, social media, enz.

Information Security Information Management System (ISMS): deel van het gehele managementproces dat zorg draagt voor de planning, implementatie, het onderhoud, de beoordeling, en het verbeteren van Privacy & Security.

Integriteit: kwaliteitseis aan data/informatie en systemen/applicaties die moet verzekeren dat de data/informatie en systemen/applicaties alleen op voorgeschreven wijze kunnen worden gewijzigd door bevoegde personen.

Labeling: het toevoegen van een (digitaal) 'etiket' aan documenten waaruit de gevoeligheid voor onbevoegde bekendmaking blijkt.

Persoonsgegevens: gegevens die ofwel direct over iemand gaan, ofwel (zonder al te veel moeite) naar deze persoon te herleiden zijn.

Privacy: de bescherming en beveiliging van de persoonsgegevens die VfPf gebruikt.

Security: de beveiliging van alle soorten van informatie die VfPf gebruikt.

Systemen: de technische omgeving waarmee de gewenste businessfunctionaliteit wordt geleverd.

Vertrouwelijkheid: kwaliteitseis aan data/informatie en systemen/applicaties die moet verzekeren dat alleen bevoegde personen toegang hebben tot de data/informatie en systemen/applicaties.