Toezichtplan FG 2022

RUD UTRECHT

Inhoud

1. Inleiding

De RUD Utrecht heeft de verantwoordelijkheid ten aanzien van Privacy belegd bij de FG in het team bedrijfsvoering. Onder aansturing van de manager bedrijfsvoering. Vanwege beperkte capaciteit en het niet beschikken over een Privacy officer zijn de verschillende taken op uitvoeringsniveau belegd bij verschillende adviseurs binnen de organisatie.

De RUD Utrecht heeft een 10tal BOA's in dienst die voor hun strafrechtelijks zaken niet vallen onder de AVG maar onder het regime van de Wpg.

Doelstelling van de RUD Utrecht is om door te groeien naar volwassenheidsniveaus met betrekking tot twee normenkaders: de BIO voor informatieveiligheid en de privacy baseline van het Centrum Informatiebeveiliging en Privacy voor privacy. Toezicht op deze werkzaamheden wordt gehouden door diverse adviseurs informatieveiligheid, de Bevoegd Functionaris in het kader van de WPG en door de Functionaris voor Gegevensbescherming voor privacy. Daar waar onderwerpen beide onderwerpen betreffen vindt samenwerking plaats tussen de adviseurs en de FG.

Volwassenheidsniveau 3 CIP

Het CIP heeft een systeem beschreven van verschillende volwassenheidsniveaus met de bijbehorende maatregelen om de volwassenheid van een organisatie op het gebied van privacy te beschrijven. Dit systeem helpt organisaties te groeien naar het volwassenheidsniveau dat past bij de visie en de missie van de organisatie ten aanzien van de privacybescherming. Er worden 5 volwassenheidsniveaus onderscheiden, grofweg van geen of versnipperde aandacht voor privacy, tot perfecte organisatie brede beheersing en benutting van de privacybescherming. Een niveau geeft daarbij de mate aan, waarin de 'organisatie van privacy' is gesystematiseerd en geïnternaliseerd in de organisatie.

Het CIP geeft aan dat op voorhand niveau 3 een redelijk volwassenheidsniveau is voor organisaties die persoonsgegevens verwerken. Het is doorgaans voldoende om de compliance-toets te doorstaan en het is ook een niveau dat voor grotere en kleinere organisaties alleszins haalbaar is.

De RUD Utrecht heeft zich tot doel gesteld te groeien naar volwassenheidsniveau 3. Binnen de RUD worden veel persoonsgegevens verwerkt van burgers, bedrijven en personeel. Waarbij ook gevoelige of bijzondere persoonsgegevens zijn, zoals personeelsgegevens, camerabeelden en strafrechtelijke gegevens. Te werken naar volwassenheidsniveau 3 is daarmee voor nu proportioneel.

Opgemerkt wordt dat het behalen van het gestelde volwassenheidsniveau niet betekent dat het daarna 'klaar' is. Om dit niveau te handhaven is continu aandacht en inzet nodig om ontwikkelingen bij te houden.

Door middel van een self assessment kan worden vastgesteld wat het thans geldende volwassenheidsniveau is. De schatting is dat we nu ergens tussen 1 en 2 staan. Door dit assessment jaarlijks te herhalen kan worden bepaald welke activiteiten nodig zijn om het gewenste niveau te halen. Door regelmatig de voortgang te bespreken binnen het cluster IV kan de FG toezicht houden op de uitvoering van de werkzaamheden en daarbij tijdig signaleren wanneer de werkzaamheden niet (meer) volgens planning verlopen.

In dit toezichtjaarplan worden deze werkzaamheden beschreven. Daarnaast wordt beschreven op welke aspecten binnen het toezicht het komende jaar de nadruk wordt gelegd.

2. Rol en taken FG

De FG is een onafhankelijke toezichthouder die binnen de organisatie toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming en de Wet politiegegevens. De taken van de FG bestaan kort gezegd uit informeren en adviseren van de organisatie en de werknemers over de AVG en voor de BOA's de Wpg, toezien op de naleving van de AVG en Wpg, adviseren over Data Protection Impact Assessments en optreden als aanspreekpunt voor de Autoriteit Persoonsgegevens.

Om deze taken goed te kunnen uitvoeren is in de AVG vastgelegd dat de FG toegang moet krijgen tot alle informatie die de FG hierbij nodig heeft. Ook mag de FG niet benadeeld of ontslagen worden voor het uitvoeren van zijn/haar taken. Daarnaast brengt de FG rechtstreeks verslag uit aan de hoogste leidinggevende gremia van de organisatie. Voor de RUD Utrecht zijn dat het MT en DB. Daarbij zal ook het AB geïnformeerd worden middels een jaarverslag.

In dit toezichtplan worden deze – algemeen beschreven taken – uitgewerkt in meer concrete werkzaamheden en wordt toegelicht waar de focus van het toezicht zal liggen in het kalenderjaar 2022.

3. Reguliere werkzaamheden

Naast het toezicht op de aandachtsgebieden bestaat het werk van de FG uit diverse werkzaamheden om het contact met de organisatie te houden en zo risicovolle situaties te signaleren, te adviseren op proces overstijgende verwerkingen en zichtbaar te zijn. Ook stimuleert de FG de samenwerking met de collega's van informatieveiligheid om een complete risicoanalyse te kunnen geven. Om deze doelen te bereiken neemt de FG deel aan diverse inhoudelijke overleggen. Ook de beoordeling van DPIA's en daarmee van de privacy risico's van de RUD is onderdeel van de werkzaamheden. Hieronder een – niet uitputtend – overzicht van de regulieren werkzaamheden.

Het toezicht door de FG bestrijkt de gehele organisatie, voor zover het gaat om de verwerking van persoonsgegevens. Binnen de organisatie worden heel veel processen uitgevoerd, met daarbinnen talrijke verwerkingen van persoonsgegevens (zoals de verzameling, uitwisseling en opslag van die gegevens). Dit jaar worden alle processen in kaart gebracht om voor de komende jaren de

onderdelen te kunnen selecteren waar de meeste risico's zitten. Alle onderdelen komen dan in 5 jaar tijd aan de orde.

Het is onmogelijk om als FG aan al die verwerkingen evenveel tijd en aandacht te geven. Daarom wijst de FG ieder jaar enkele aandachtgebieden aan. Hieronder worden deze aandachtsgebieden nader uitgewerkt.

a) Uitvoeren en opvolgen DPIA's

Een data protection impact assessment is een instrument om privacy risico's binnen een proces of project vast te stellen. Om deze risico's terug te brengen naar een acceptabel niveau worden in de DPIA aanbevelingen opgenomen. Het opvolgen van deze aanbevelingen valt onder de verantwoordelijkheid van de proceseigenaar.

In de afgelopen jaren heeft de focus vooral gelegen op het voldoen aan de AVG en WPG en zijn er geen DPIA's uitgevoerd. De autoriteit Persoonsgegevens heeft een lijst samengesteld van verplichte onderwerpen waarvoor een DPIA moet worden uitgevoerd. Daarom wordt er dit jaar en volgend jaar extra nadruk gelegd op het uitvoeren van een aantal van deze verplichte DPIA's.

b) Bewustwording en voorlichting

Het vergroten van het bewustzijn en het voorlichten van medewerkers op het gebied van privacy en informatieveiligheid is een doorlopende basisvoorwaarde voor de naleving van de AVG. Daar waar geen kennis is, kan immers ook geen naleving van regels worden verwacht. In 2021 is op Viadesk regelmatig aandacht besteed aan Privacy isseus waaronder waarschuwingen voor phishing mails en aandacht voor privacy en thuiswerken en het doen van meldingen van datalekken. Dit blijft ook de komende jaren een aandachtpunt.

c) In kaart brengen alle processen

Dit jaar worden alle processen die van toepassing zijn in kaart gebracht. Na het in kaart brengen van de processen kan per jaar een selectie worden gemaakt om toezicht op uit te voeren. Hiermee krijgt het toezichtplan een meer strategisch karakter en kan in roulatie alle processen eens in de 5 jaar orden gecontroleerd.

Actie	Wanneer	Product
In kaart brengen van alle processen	Q4	Overzicht processen
De aandachtpunten en verbeterpunten die voortvloeien uit de Wpg audit	Voor Q4	Interne audit
Het uitvoeren en afronden van DPIA's: Dashcams en wildcamera's, zaaksysteem en gebruik drones.	Q2	DPIA adviezen
Het uitvoeren van privacy-by-design en privacy-by-default voor de ontwikkeling van app's	Q3	
Opzetten van een intern audit programma Wpg	Q2	Auditplanning
Maken toezichtplan van FG	Q2	Toezichtplan
Blijvende aandacht voor bewustwording van medewerkers	continue	

Lijst afkortingen

AVG Algemene verordening gegevensbescherming

Wpg Wet politiegegevens

FG Functionaris voor de Gegevensbescherming

BOA Buitengewoon Opsporings Ambtenaar

BIO Baseline informatiebeveiliging Overheid

CIP Centrum Informatiebeveiliging en Privacybescherming

DPIA Data Protection Impact Assessments

Ciso chief information security officer