AVG PROTOCOL

(GDPR)

CertiFlex

De Huufkes 104

5674 TM Nuenen

Document nummer: 000

Versie nummer: 003

1-3-2020

Opgesteld door: M. Staring

Kwaliteitsmanager en (Anti-) Fraudefunctionaris CertiFlex

D.d. 01-03-2020

Inhoudsopgave:

Inleiding / Voorwoord:

Op 25 mei 2018 verandert er veel op het gebied van privacybescherming. Op die datum wordt de oude Wet Bescherming Persoonsgegevens (WBP) definitief vervangen voor de Algemene Verordening Gegevensbescherming (AVG), ook wel bekend als de General Data Protection Regulation (GDPR).

De AVG is een Europese richtlijn die op 25 mei 2016 binnen alle lidstaten van de Unie in werking is getreden. De overheid heeft alle organisaties twee jaar de tijd gegeven om de bedrijfsvoering voor te bereiden op deze nieuwe richtlijn. 25 mei 2018 is de harde deadline geworden en vanaf die datum kunt u dan ook worden aangesproken op uw verantwoordelijkheid. Als na die datum blijkt dat u het met de naleving niet zo nauw heeft genomen, kan een boete opgelegd worden.

Dit (AVG) Protocol is bedoeld om (U) een zo volledig mogelijk, maar vooral ook een praktisch en realistisch, beeld te geven van wat er verandert en wat dat mogelijk voor U betekent.

Waarom de AVG?

Tot 25 mei 2016 had elke lidstaat binnen de Europese Unie een eigen privacywetgeving die meestal gebaseerd was op de Europese privacyrichtlijn uit 1995. Deze Europese privacyrichtlijn stamt uit de tijd dat het internet nog in de kinderschoenen stond. Er werd geen rekening gehouden met de enorme toename in risico's en dreigingen die hand in hand gingen met enorme groei van onlineactiviteiten. Bovendien was het voor bedrijven met vestigingen in andere Unielanden vaak lastig om in alle gevallen goed te voldoen aan afwijkende nationale privacyrichtlijnen. Die konden immers per lidstaat verschillen.

Doel

Doel van de AVG is te zorgen voor harmonisatie en versterking van de bescherming van persoonsgegevens binnen de Europese Unie.

CertiFlex relatie t.a.v. de AVG?

-Diverse overeenkomsten, w.o. met de CBI's
-Overige instanties, (w.o. Persoonscertificatie),
-Opdrachtgevers / Klanten, w.o. de Opleidingsinstituten,
-Leveranciers,
-Examinatoren,
-Kandidaten,
-Personeelsdossiers, (Medewerkers CertiFlex en Examinatoren),

Wat houdt de AVG precies in?

Er gaat op het internet veel informatie rond over de AVG. Artikelen waarin de focus vooral ligt op de eisen met betrekking tot de bescherming van persoonsgegevens en de sancties als blijkt dat aan die eisen niet voldaan wordt. Wat bijzonder is, is dat de AVG helemaal niet bedoeld is om de privacy te beschermen. Privacy is namelijk een grondrecht dat wordt geborgd in zowel de Nederlandse als de Europese Grondwet en is vanuit de Grondwet bijna als vanzelf voldoende beschermd.

De Nederlandse Grondwet zegt het volgende:

Artikel 10 lid 1: “Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer”.

De Europese Grondwet is daarover nog duidelijker:

Artikel II-68 lid 1: “Eenieder heeft recht op bescherming van zijn persoonsgegevens”.

De AVG is niet zozeer bedoeld om de privacy te beschermen maar veel meer bedoeld om een veilig kader te bieden waarbinnen inbreuk op dat grondwettelijk recht mogelijk wordt gemaakt. Daarom is artikel 1 van de AVG ook een belangrijk artikel om in gedachten te houden bij alle verdere overwegingen met betrekking tot de AVG.

Artikel 1 van de AVG luidt als volgt:

Hoofdstuk Algemene bepalingen, artikel 1

Onderwerp en doelstellingen

1. Bij deze verordening worden regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van persoonsgegevens.

2. Deze verordening beschermt de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.

3. Het vrije verkeer van persoonsgegevens in de Unie wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens.

4. Met name het derde punt is in de context van dit document van belang. De AVG erkent namelijk het recht op privacy maar stelt tegelijkertijd dat het vrij verkeer van persoonsgegevens niet beperkt of verboden mag worden! Zonder vrij verkeer van persoonsgegevens is sociaal verkeer bijna onmogelijk en kunnen veel dienstverleners geen diensten meer aanbieden of overeenkomsten sluiten. Kortom, inbreuk plegen mag, maar alleen als u daarbij het grondrecht in gedachten houdt.

5. Wie aan de letter van de wet wil voldoen, voelt nu waarschijnlijk nattigheid. De letter van de wet spreekt zichzelf immers min of meer tegen. Dit brengt ons tot wat de AVG nu precies inhoudt: de AVG is vooral bedoeld om u te helpen bij het maken van de juiste afwegingen tussen zakelijke belangen enerzijds en het recht op privacy van natuurlijke rechtspersonen anderzijds. En om die afweging goed te maken, is het belangrijk dat u de uitgangspunten van de AVG goed in gedachten houdt.

Wat zijn de belangrijkste overwegingen in de AVG?

De AVG is bedoeld om privacyrechten van natuurlijke personen uit te breiden en te versterken en legt meer verantwoordelijkheid rond de verwerking van die gegevens bij de verwerkende organisaties. In hoofdstuk II artikel 5 zijn de beginselen inzake de verwerking van persoonsgegevens vastgelegd.

Dit zijn de uitgangspunten uit artikel 5 van de AVG:

• Transparantie: helder voor alle betrokkenen
• Doelbeperking: de persoonsgegevens worden voor een welbepaald gewettigd doel verzameld en mogen niet voor andere zaken gebruikt worden
• Gegevensbeperking: enkel de noodzakelijke gegevens die voor het beoogde doel noodzakelijk zijn, mogen worden verzameld
• Juistheid: de persoonsgegevens moeten correct zijn en blijven
• Bewaarbeperking: de persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel
• Integriteit en vertrouwelijkheid: de persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging
• Verantwoording: de verantwoordelijke moet kunnen aantonen aan deze regels te voldoen

Deze beginselen vertalen zich naar een aantal praktische voorwaarden die er als volgt uitzien:

Transparantie

De AVG vraagt niet alleen dat u voor uzelf helder moet hebben waar en om welke reden u persoonsgegevens verzamelt en verwerkt maar ook dat u dit laat weten aan diegene van wie u gegevens verwerkt. Bovendien moet u diegene informeren over wat zijn/haar rechten zijn en hoe die rechten uit kunnen worden geoefend.

Dit wordt gedaan middels het zogenaamde Inschrijfformulier.

Doelbeperking

Het doel waarvoor u persoonsgegevens verzamelt en verwerkt moet een wettige basis hebben en mag niet zomaar veranderen. **Artikel 6 van de AVG** geeft een aantal duidelijke grondslagen voor de rechtmatigheid van verwerking. Is geen van die grondslagen van toepassing, dan mag u de gegevens niet verzamelen en verwerken.

Gegevensbeperking

U mag niet meer (kandidaat) gegevens verzamelen dan u nodig heeft om uw doelen te bereiken. Uw doelen zijn de redenen waarom u persoonsgegevens verzamelt zoals u die heeft omschreven om transparantie te kunnen borgen. Vervalt het doel dan moet u de verwerking staken. Verandert het doel dan moet u goed nagaan of de nieuwe doelstelling te verenigen is met de oorspronkelijke doelstelling. Is dat niet het geval dan moet u de verwerking staken.

Maximale (gewone) kandidaat gegevensverwerking CertiFlex:

1) Kandidaat nummer,
2) Naam, Voornaam, Roepnaam,
3) Alle voorletters,
4) Tussenvoegsel, en of anders,
5) Achternaam,
6) Straat,

7) Huisnummer en of letter,
8) Postcode
9) Woonplaats,
10) Geboortedatum,
11) Geboorteplaats
12) Mailadres,
13) Pasfoto,
14) Rekeningnummer,

Maximale (bijzondere) kandidaat gegevensverwerking CertiFlex:

1) Taal t.a.v. de VCA B en VCA VOL Examens, (28 talen + Arabisch),
2) Taal t.a.v. TCVT / TCVT-RA (4 talen),
3) BSN / BurgerServiceNummer (I.v.m. de zogenaamde ‘’Asbest’’ Examens)
4) VCA-diplomanummer (indien het een VCA/SOG opleiding betreft)

Maximale (gewone) personeels (Examinator) gegevensverwerking CertiFlex:

1) Naam, Voornaam, Roepnaam,
2) Alle voorletters,
3) Tussenvoegsel, en of anders,
4) Achternaam,
5) Straat,
6) Huisnummer en of letter,
7) Postcode
8) Woonplaats,
9) Geboortedatum,
10) Geboorteplaats
11) Mailadres,
12) Pasfoto,
13) Rekeningnummer,
14) Rijbewijs(en),
15) Telefoonnummer (vast),
16) Telefoonnummer (mobiel),
17) Opleidingsniveau,
18) Gevolge cursussen,
19) Stages,
20) Arbeidsverleden,

Maximale (bijzondere) personeels (Examinator) gegevensverwerking CertiFlex:

21) Geslacht,
22) Nationaliteit,
23) Taal t.a.v. de VCA B en VCA VOL Examens, (28 talen + Arabisch),
24) Taal t.a.v. TCVT / TCVT-RA (4 talen),
25) BSN / BurgerServiceNummer (I.v.m. de Belastingdienst) /
    en i.v.m. de zogenaamde ‘’Asbest’’ Examens
26) VCA-diplomanummer (I.v.m. VCA/SOG)

Note: Andere kandidaat / personeels (Examinatoren) gegevens worden er niet verwerkt bij CertiFlex.

Maximale gegevens bedrijf / instelling / organisatie gegevensverwerking CertiFlex

1) Gegevens bedrijf
2) Naam bedrijf
3) Bezoekadres
4) Adres/Postcode/-plaats
5) Postadres
6) Postcode/-plaats
7)Telefoonnummer
8) Contactpersoon
9) Naam contactpersoon
10) Mobiel telefoonnummer
11) E-mailadres
12) E-mailadres voor digitale facturatie
13) IBAN-nummer
14) KVK-nummer
15) BTW-nummer
16) Factuur wordt betaald door Opmerkingen/Inkoopnummer/Ordernummer (Tegenbon)

Note: Andere ‘’bedrijfs’’gegevens worden er niet verwerkt bij CertiFlex.

Juistheid

Bij de verwerking van persoonsgegevens moet u alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens die u verzamelt juist zijn. Indien nodig dienen deze gegevens te worden aangepast of verwijderd als zij niet kloppen.

Note: CertiFlex heeft hiervoor diverse controle momenten ingebouwd.

T.a.v. een VCA Examen:
(Controles uitgevoerd door de Examinator!)
-Controle d.m.v. I.D. in combinatie met de Presentielijst.
-Controle tijdens het VCA Examen moment, de ID ligt immers rechtsboven op de tafel van de desbetreffende Examenkandidaat,
-Controle aan het einde van het VCA Examen,

Bovenstaande is conform het: VCAInfra Handboek / VCA eis.

Bewaarbeperking

U dient de bewaartermijn van persoonsgegevens te beperken tot een termijn die in redelijkheid overeenstemt met het doel waarvoor u die gegevens verzameld hebt. U mag dus persoonsgegevens bewaren als dat nodig is om te voldoen aan andere wettelijke verplichtingen zoals bijvoorbeeld de administratieplicht. Integriteit en vertrouwelijkheid U neemt technisch en organisatorisch zodanig maatregelen dat een passende beveiliging gewaarborgd kan worden. U zorgt ervoor dat gegevens alleen toegankelijk zijn voor diegenen die deze gegevens nodig hebben voor verwerking en dat de gegevens beschermd zijn tegen onopzettelijk verlies of diefstal.

Administratie CertiFlex

Wettelijke bewaartermijnen:

Onze overheid stelt wettelijke verplichtingen omtrent diverse bewaartermijnen, te weten:

Processen:	Maximale bewaartermijn:	Grondslag:
Sollicitatieprocedure	1 jaar + 2 maanden	Vrijstellingsbesluit WBP
Indiensttreding arbeidsovereenkomst	Actief in dienst+7 jaar	Wet op de Rijkbelastingen
Verzuimbeheer	2 jaar	Vrijstellingsbesluit WBP
Beveiligingscamera's	4 weken	Vrijstellingsbesluit WBP
Bezoekersregistratie	6 maanden	Vrijstellingsbesluit WBP
Logging internetgebruik, netwerk	6 maanden	Vrijstellingsbesluit WBP
Gerechtelijke procedures	2 jaar	Vrijstellingsbesluit WBP
(Examen) Kandidaat TCVT(-RA)	5 jaar + 2	Zelf vastgesteld
(Examen)Kandidaat VCA	10 jaar + 2	Zelf vastgesteld
(Examen)Kandidaat Asbest	3 jaar + 2	Zelf vastgesteld
Examinatoren	10 jaar + 2	Zelf vastgesteld
Klantcontactmanagement	5 jaar	Zelf vastgesteld
Salarisafspraken en arbeidsvoorwaarden	7 jaar	Wet op de Rijkbelastingen
Loonbelasting en identiteitsbewijzen	5 jaar	Uitvoeringsregeling LB
Debiteuren- en crediteurenadministratie	7 jaar	Wet op de Rijkbelastingen

Note: Lees voor examinator / Personeel en:

(Dag-)Voorzitters, Examinatoren, Examenleiders, Toezichthouders, Surveillanten, Enz. Etc,

Hebben een zogenaamde: Verwerkersovereenkomst (CertiFlex) getekend. Deze overeenkomst is opgeslagen in de Personeelsdossiers.

Verwerkersovereenkomst.

Verantwoording

De toezichthouder verwacht van u dat u kunt aantonen dat u de nodige inspanningen hebt verricht om aan de AVG te kunnen voldoen. Zorg daarom voor een helder beschreven privacy beleid (Dit AVG Protocol) en zorg dat uw personeel getraind is. (Geïnstrueerd) Leg goed vast welke gegevens u verzamelt voor welke doeleinden en hoe lang u die gegevens bewaart.

AVG en de ISO 9001:2015 CertFlex

In het Handboek van CertiFlex zijn passages van het AVG Protocol verwerkt.

Vernietiging (Persoons-)Gegevens

Is de bewaartermijn van (persoons-)gegevens verstreken of zijn de gegevens niet meer noodzakelijk voor het doel? Dan moeten de gegevens vernietigd worden. Denk bijvoorbeeld aan gegevens over loonbeslag als het loonbeslag is opgeheven. Vernietiging moet gebeuren onder controle van uw bedrijf. Vernietigen houdt in dat de gegevens niet langer meer bestaan of niet langer meer bestaan in een bruikbare vorm.

Vernietiging (Persoons-en Bedrijfs) Gegevens / Cyclus

Bij CertiFlex is daarvoor de volgende cyclus opgezet, omdat de AVG geen extra eisen stelt aan de vernietiging van (persoons-)gegevens.
Er is een afgesloten beveiligde archiefvernietigingscontainer.
CertiFlex ontvangt een factuur en een vernietigingscertificaat van de (versnipperde) inhoud.
Er is een vernietigingsregistratiedocument waarop door de vernietiger wordt aangegeven welk document c.q. dossier wordt vernietigd, d.m.v. het noteren van het document c.q. dossiernummer en de vernietigingsdatum, en een paraaf van de vernietiger.
CertiFlex ontvangt een factuur en een vernietigingscertificaat van de (versnipperde) inhoud.
Na elke leging van de archiefvernietigingscontainer wordt er met een nieuw vernietigingsregistratiedocument aangevangen. Het oude ingevulde document wordt gearchiveerd, samen met het vernietigingscertificaat.
Zo ontstaat er een betrouwbare geschiedenis van de vernietigde documenten.

Uiteenschrijving 10 Aandachtpunten

De hierboven genoemde aandachtspunten worden een voor een hieronder uitgeschreven in een praktische Checklist van 10 Hoofdpunten.

Aandachtspunt 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven, zoals guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Note: Duidelijk.

Aandachtspunt 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Bereid u daar op voor zodat u op tijd en op de juiste manier op verzoeken reageert.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Note: Zie de Algemene Voorwaarden van CertiFlex.

Aandachtspunt 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt. Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt.

U kunt het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Vermeld in het overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt. Beroept u zich bijvoorbeeld op een gerechtvaardigd belang of vraagt u toestemming aan de betrokkenen? NB: de grondslagen in de AVG zijn grotendeels hetzelfde als die in de huidige Wbp.

Note: Inschrijfformulier.

Aandachtspunt 4: Data protection impact assessment

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Note: Dit is niet het geval.

Aandachtspunt 5: Privacy by design & privacy by default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van privacy by design en privacy by default en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

- een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is;
- op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken;
- als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Note: Duidelijk.

Aandachtspunt 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen. Bepaal nu alvast of dit voor uw organisatie geldt. Zo ja, wacht dan niet te lang met het werven van een FG. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Note: Het aanstellen van een FG is (nu) niet aan de orde.

Aandachtspunt 7: Meldplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

Note: Conform Handboek CertiFlex.

Aandachtspunt 8: Bewerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een bewerker (in de AVG ‘verwerker’ genoemd)? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Note: Met diverse partijen is een overeenkomst van toepassing. (Opdrachtgevers / Leverancier).

Aandachtspunt 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Note: Niet van toepassing zijnde.

Aandachtspunt 10: Toestemming

Voor sommige gegevensverwerkingen hebt u toestemming nodig van de betrokkenen. De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Pas deze wijze indien nodig aan. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Note: Middels tekst op het aanmeldformulier / Aanstellingsovereenkomst Examinator.

Toestemming foto’s / Website

CertiFlex heeft op haar Website en of anders geen foto’s staan van derden.

Toestemming camerabeelden

CertiFlex heeft geen camerasystemen, en verwerkt zo ook geen camerabeelden.

Uiteenschrijving CertiFlex maatregelen:

Stap 1: Bewustwording

Zorg ervoor dat de relevante mensen in uw organisatie (zoals beleidsmakers) op de hoogte zijn van de nieuwe privacyregels. Zij moeten inschatten wat de impact van de AVG is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen. Houd er rekening mee dat de implementatie van de AVG veel kan vragen van de beschikbare menskracht en middelen en begin er daarom op tijd mee.

De Autoriteit Persoonsgegevens (AP) biedt instrumenten die u kunnen helpen om de AVG na te leven. Zoals de website hulpbijprivacy.nl en de AVG-regelhulp. Maar ook guidelines die zijn opgesteld samen met de andere privacytoezichthouders in Europa.

Note: Duidelijk.

Stap 2: Rechten van betrokkenen

Onder de AVG krijgen de mensen van wie u persoonsgegevens verwerkt meer en verbeterde privacyrechten. Zorg er daarom voor dat zij hun privacyrechten goed kunnen uitoefenen.

Denk daarbij aan bestaande rechten, zoals het recht op inzage en het recht op correctie en verwijdering. Maar houd ook alvast rekening met nieuwe rechten, zoals het recht op dataportabiliteit. Bij dit recht moet u ervoor zorgen dat betrokkenen hun gegevens makkelijk kunnen krijgen en vervolgens kunnen doorgeven aan een andere organisatie als ze dat willen.

Ook kunnen mensen bij de AP klachten indienen over de manier waarop u met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

Note: Ook CertiFlex beschikt over een zogenaamde ‘’Klachtenprocedure’’ echter spreken wij liever van een verbeterprocedure en een Verbeterformulier.

Stap 3: Overzicht verwerkingen

Breng uw gegevensverwerkingen in kaart. Documenteer welke persoonsgegevens u verwerkt en met welk doel u dit doet, waar deze gegevens vandaan komen en met wie u ze deelt.

Onder de AVG heeft u een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. Het bijhouden van een register van verwerkingsactiviteiten is onderdeel van de verantwoordingsplicht.

U kunt het register ook nodig hebben als betrokkenen hun privacyrechten uitoefenen. Als zij u vragen hun gegevens te corrigeren of verwijderen, moet u dit doorgeven aan de organisaties waarmee u hun gegevens heeft gedeeld.

Note: Gegevens worden met de hieronder genoemde partijen gedeeld:

Register:

TriFact365	Facturen	Diverse
DNV-GL	Persoonscertificatie	TCVT / Asbest
TCVT / TCVT-RA	Persoonscertificatie	TCVT / TCVT-RA
SSVV (VCA-SOG)	Persoonscertificatie	VCA en SOG
Scab	Salarisadministratie	Personeel

Stap 4: Data protection impact assessment

Onder de AVG kunt u verplicht zijn een zogeheten data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt. U kunt nu alvast inschatten of u straks DPIA's moet uitvoeren en hoe u dit dan gaat aanpakken.

Komt straks uit een DPIA naar voren dat uw beoogde verwerking een hoog risico oplevert? En lukt het u niet om maatregelen te vinden om dit risico te beperken? Dan moet u met de AP overleggen voordat u met de verwerking start. Dit wordt een voorafgaande raadpleging genoemd. De AP beoordeelt dan of de voorgenomen verwerking in strijd is met de AVG. Is dit het geval, dan ontvangt u een schriftelijk advies van de AP.

Note: Er worden geen hoog risico gegevens verwerkt. DPIA Is niet uitgevoerd, wel besproken.

Stap 5: Privacy by Design & Privacy bij Default

Maak uw organisatie nu al vertrouwd met de onder de AVG verplichte uitgangspunten van privacy by design en privacy by default en ga na hoe u deze beginselen binnen uw organisatie kunt invoeren.

Privacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. Maar bijvoorbeeld ook dat u niet meer gegevens verzamelt dan noodzakelijk voor het doel van de verwerking. En dat u de gegevens niet langer bewaart dan nodig.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld door:

• een app die u aanbiedt niet de locatie van gebruikers te laten registeren als dat niet nodig is; • op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aan te vinken; • als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens te vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensbescherming (FG) aan te stellen. Voor de organisatie CertiFlex is het niet perse noodzakelijk om zo'n functionaris aan te stellen.

Note: Wel beschikt zij over een (Anti-) Fraudefunctionaris.

Stap 7: Meldingsplicht datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in de organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Dit gaat verder dan de huidige protocolplicht uit de Wbp, die alleen betrekking heeft op de gemelde datalekken.

De Europese privacytoezichthouders hebben in oktober 2017 guidelines gepubliceerd over de meldplicht datalekken onder de AVG.

Note: Van bovenstaande hebben wij notitie genomen, indien er zich in de toekomt een datalek optreedt zal de directie in overleg met de (Anti)Fraudefunctionaris passende maatregelen nemen.

Note: Zie Handboek CertiFlex.

Deze guidelines zijn nog niet definitief, maar staan open voor publieke consultatie. Wanneer de guidelines definitief zijn, kunnen wij de volledige informatie over de meldplicht datalekken onder de AVG tot ons nemen.

Stap 8: Verwerkersovereenkomsten

Heeft u uw gegevensverwerking uitbesteed aan een verwerker? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw verwerkers nog steeds toereikend zijn. En of deze voldoen aan de eisen die de AVG aan verwerkersovereenkomsten stelt. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Note: Verwerkersovereenkomsten zijn uitgezet.

Stap 9: Leidende toezichthouder

Heeft uw organisatie vestigingen in meerdere EU-lidstaten? Of hebben uw gegevensverwerkingen in meerdere lidstaten impact? Dan hoeft u onder de AVG nog maar met één privacytoezichthouder zaken te doen. Dit wordt de leidende toezichthouder genoemd. Geldt dit voor uw organisatie, bepaal dan onder welke privacytoezichthouder u valt.

Note: N.v.t.

Stap 10: Toestemming

Voor sommige gegevensverwerkingen hebben wij toestemming nodig van de betrokkenen. (Bijv. van examenkandidaten) De AVG stelt strengere eisen aan toestemming. Wij monitoren en evalueren daarom de manier waarop wij toestemming vragen, krijgen en registreren. Indien nodig passen wij deze wijze aan. Nieuw is dat wij moet kunnen aantonen dat wij geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor mensen net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven.

Note: Zie onderschrift aanvraag Examenformulier CF000FOR000

Organisatorische maatregelen

We besteden veel aandacht aan awareness over privacy en informatiebeveiliging. Iedereen die bij ons werkt, moet een geheimhoudingsverklaring tekenen en krijgt indien gewenst interne trainingen over veiligheid en privacy.

Ook evalueren we continu onze interne procedures en processen. Toegang tot CertiFlex data is gelimiteerd en er vindt voortdurende monitoring op toegang tot CertiFlex data plaats. We hebben een streng intern autorisatie- en authenticatiebeleid dat we periodiek evalueren.

Externe Audits

-Jaarlijks wordt CertiFlex door minimaal vijf externe partijen geaudit, te weten:

-BSI, Extern Auditbureau: Audit op de ISO 9001: 2015 Certificatie,

-DNV-GL, t.a.v. Asbest Examens / Audit op het gehele proces,

-TCVT / TCVT-RA Uitgevoerd door / namens de Examenkamer,

-KIWA, SOOB subsidie,

-SSVV, t.a.v. de VCA-SOG Examens / Audit op de procesbeheersing,

Technische maatregelen / IT beveiliging

Het liefst willen we niet te veel kwijt over hoe bij CertiFlex de persoonsgegevens zijn beveiligd, want dat geeft derden met kwade bedoelingen te veel inzicht in de beveiliging. Maar helemaal niets zeggen en u te vragen ons te vertrouwen op onze blauwe ogen is ook weer zo iets.. Daarom toch een tipje van de sluier.

Back-ups

Er worden bij CertiFlex periodiek, meerdere en uitgebreide back-ups van alle data van CertiFlex. Dit bewaren we op meerdere, *top secret* locaties zodat we data terug kunnen zetten mocht er iets gebeuren met de data van CertiFlex.

Data CertiFlex in Nederland

De CertiFlex systemen zijn dedicated intern gebouwd. Wij zijn ons bewust van de juridische implicaties van de Amerikaanse Patriot Act. We maken daarom bij CertFlex geen gebruik van cloudopslagdiensten van derden, zoals Amazon Web Services. Het CertiFlex-park staat op eigen, Nederlandse servers in onze eigen, private cloud, wat de interne controle hierop efficiënt en effectief maakt.

Clean Desk Policy

D.m.v. de vijf keer S

Het kost misschien even wat tijd om alle werknemers te laten wennen aan het feit dat ze aan het eind van de dag een paar minuten de tijd moeten nemen om hun bureau leeg te halen, maar na een tijdje is het vaste prik. De volgende 5 stappen helpen ons daarbij op weg, daarbij dienen ‘’gevoelige’’ (AVG gerelateerde) documenten zo wie zo opgeruimd te worden.

1. **Scheiden**
   Bekijk alles wat op het bureau ligt en kies: bewaren of weggooien. Zo wordt er direct onderscheidt gemaakt tussen wat echt belangrijk is en wat niet. Een belangrijke eerste stap naar een opgeruimd bureau.

2. **Schikken**
   Geef spullen een vaste plek. Dat maakt het opruimen aan het eind van de dag een stuk gemakkelijker.

3. **Schoonmaken**
   Een leeg bureau is gemakkelijker schoon te maken én te houden.

4. **Standaardiseren**
   De stap die de meeste discipline vraagt is die van het standaardiseren. Door deze stap wordt het proces van de eerste drie stappen een gewoonte.

5. **Systematiseren**
   Check eens in de zoveel tijd of de procedures ook door alle werknemers worden nageleefd.

Examendossiers

Examendossiers verblijven in speciaal afgesloten koffers zo kort mogelijk als mogelijk is. Onderweg van CertiFlex naar de Examinator en V.V. De koffers worden nooit onbewaakt, of alleen gelaten. In de overeenkomst tussen CertiFlex en de Examinator zijn daarover ook afspraken vastgelegd.

Stand der Techniek / Stand der Wetenschap

Dit AVG Protocol is met de grootst mogelijke zorgvuldigheid opgesteld. Echter, is aan de tand des tijds onderhevig, minimaal jaarlijks of zoveel keer als nodig is updaten.

Wijzigingen

Als er na 25 Mei 2018 veranderingen zijn, dient CertiFlex een PIA (Privacy Impact Analyse) uit te voeren om te bepalen of aanvullende maatregelen nodig zijn.

Analyse van de (bedrijfs-)risico's:

Dit AVG Protocol is de eerste aanzet tot AVG 25 Mei 2018.
Wij zijn van mening dat dit document in eerste instantie voldoende invulling geeft aan het correct uitvoeren van de AVG per 25 Mei 2018. Ons inzien zijn de zogenaamde bedrijfsrisico's voldoende in kaart gebracht en geanalyseerd, mede ondersteund door het Handboek CertiFlex.

Afkortingen:

AP / Autoriteit Persoonsgegevens
Ascert / Stichting Certificering Asbest
AVG / Algemene Verordering Gegevensbescherming
BSI / Britisch Standards Institution (CertiFlex's ISO 9001:2015 Externe Certificerende instelling)
BSN / Burgerservicenummer
DNV-GL / Verwerker van de TCVT Persooncertificatie
DPIA / data protection impact assessment
DPO / Data Protection Officer = FG
FG / Functionaris Gegevensbescherming
GDPO / Guidelines on Data Protection Officers / Europese toezichthouders
GDPR / General Data Protection Regulation
Handboek CertiFlex / Dit is een Handboek waarin staat hoe CertiFlex acteert, (Opbouw conform de ISO 9001:2015 Certificering)
KIWA / Keurings Instituut voor Waterleiding Artikelen
PIA / Privacy Impact Analyse
SOG / SSVV Opleidingsgids
SOOB / Stichting Opleidings- en Ontwikkelingsfonds Beroepsgoederenvervoer
SSVV / Stichting Samenwerken voor Veiligheid
TCVT / Stichting Toezichthouder Verticaal Transport
TCVT-RA / Stichting Toezichthouder Verticaal Transport, Register Authoriteit

VCA / Veiligheid Checklist Aannemers
VCA B / VCA Basis = VCA Certificatie voor medewerkers
VCAInfra Handboek / In dit Handboek staat omschreven hoe, en wat te acteren
VCA VOL / VCA VOL = VCA Certificatie voor leidinggevende
Wbp / Wet bescherming persoonsgegevens (van 06-07-2000 tot 25-05-2018)

Note: Lees voor examinator: (Dag-)Voorzitters, Examinatoren, Examenleiders, Toezichthouders, Surveillanten, Correctors, Enz. Etc, (Examenpersoneel).

Opgesteld door: M. Staring
Kwaliteitsmanager en (Anti-) Fraudefunctionaris CertiFlex
D.d. 01-03-2020

Gecontroleerd door de Directie van CertiFlex

Einde