12 tips voor correct gebruik van TOPdesk m.b.t de GDPR

1 Registreer en communiceer gevoelige gegevens

In TOPdesk ondersteun je eenvoudig klanten, of dit nu collega's zijn of externe klanten van je organisatie. Om goede ondersteuning te bieden, is het voor aanvragen vaak nodig om contactgegevens zoals e-mailadres, telefoonnummer of adres te registreren.

De gegevens kunnen gevoelig zijn. Dit is afhankelijk van het soort diensten dat je biedt en de relatie met de betrokkene. Registreer en communiceer deze gegevens goed voor volgende stappen in je proces. Met het kennissysteem van TOPdesk deel je deze gegevens eenvoudig met behandelaars en communiceer je transparant met klanten over je gegevensverwerking.

2 Vraag toestemming van betrokkene(n)

TOPdesk wordt gebruikt voor het ondersteunen van medewerkers en directe klanten van de organisatie. Zolang de gegevens geregistreerd in TOPdesk nodig zijn voor het uitvoeren van een contract, zoals een werknemers- of klant-leverancierscontract waar de betrokkene een partij is, is het legaal om deze gegevens zonder toestemming te registreren. In andere gevallen moet je expliciet toestemming vragen aan de betrokkene(n).

3 Houd controle over toegangsgegevens

In TOPdesk kan je rechten en filters definiëren zodat alleen de mensen die toestemming mogen hebben ook echt de enigen zijn met toestemming. Het koppelen van TOPdesk aan je centrale Identity System, zoals (Azure) Active Directory, zorgt ervoor dat toegang tot TOPdesk altijd in overeenstemming is met het veiligheidsbeleid van je organisatie.

Er zijn altijd mensen betrokken bij het verwerken van gegevens. Het is belangrijk dat deze mensen weten hoe ze met deze gegevens om moeten gaan voordat ze toegang krijgen. Een training 'Bewust omgaan met gegevens' is een goede start. Bij TOPdesk hebben we een aantal voorbeelden van zulke trainingen. Onze consultants kunnen je hier altijd bij helpen.

4 Retentie van gegevens

Retentiebeleid is onderdeel van de GDPR. Dit beleid houdt in dat je moet nadenken hoelang privacygevoelige informatie beschikbaar is. Als de gegevens niet meer beschikbaar mogen zijn, dienen ze onvindbaar te zijn. Hierdoor zorg je dat het risico op het onnodig blootstellen van privacygevoelige gegevens bij een eventueel gegevenslek zo klein mogelijk is. Daarom bepaalt de GDPR ook dat 'oude' gegevens op tijd moeten worden verwijderd of onvindbaar moeten worden gemaakt voor individuen.

5 Selectie van tools en leveranciers

De Verwerkingsverantwoordelijke dient met zorg tools uit te zoeken waar gevoelige gegevens in worden geregistreerd. De verwerkingsverantwoordelijke dient in de gekozen tool zijn of haar verantwoordelijkheden rondom het verwerken van persoonlijke gegevens na te kunnen komen. Als deze tool een cloudoplossing is, omvat dit ook de geleverde diensten en managementprocessen.

Zorg ervoor dat je tijdens het selecteren van tools en leveranciers voor het verwerken van persoonlijke gegevens op de hoogte bent van de dienstenstructuur en relevante auditing rapporten. In ons ISAE 3000-auditrapport lees je welke maatregelen we hebben getroffen om een betrouwbare dienst te verlenen. Neem contact op met je accountmanager om dit rapport in te zien.

6 Overeenkomsten omtrent Gegevensbescherming

Bij SaaS is het belangrijk om een Overeenkomst omtrent Gegevensbescherming (OG) te hebben. Zo'n overeenkomst bevat duidelijke omschrijvingen van de verantwoordelijkheden van de betrokken partijen. Denk bijvoorbeeld aan een wederzijdse geheimhoudingsovereenkomst, afspraken over hoe samen te werken bij een gegevenslek, of hoe om te gaan met gegevens bij beëindiging van het dienstcontract. Zorg ervoor dat subverwerkers ook in de overeenkomstketen zitten.

TOPdesk heeft natuurlijk zelf ook contracten met relevante partijen. We gebruiken alleen datacenters die zorgen dat we onze verplichtingen richting onze klanten kunnen nakomen. Daarnaast hebben we OG's tussen alle TOPdesk-kantoren en de betrokken datacenters.

Er zijn een hoop standaardsjablonen voor Overeenkomsten omtrent Gegevensbescherming, maar het is slim om bij je leverancier na te gaan of ze een specifieke overeenkomst hebben voor hun dienstverlening. Deze specifieke overeenkomsten zijn vaak geschreven met de dienstverlening in het achterhoofd en schelen een hoop werk.

Wij hebben een OG-sjabloon beschikbaar voor onze TOPdesk SaaS-diensten. Interesse? Neem contact op met je accountmanager.

7 Recht tot herzien, correctie en 'vergeten'

Betrokkenen worden door de GDPR beschermd tegen acties van anderen. De GDPR geeft betrokkenen het recht om te herzien wat er van ze is geregistreerd. Wanneer nodig, kunnen ze vragen of de gegevens gecorrigeerd of zelfs verwijderd mogen worden.

Het is goed om je medewerkers instructies te geven hoe om te gaan met de aanvragen. In de selfserviceportal kan je laten zien wat er wordt geregistreerd. In het kennissysteem kan je documenteren welke gegevens waarom worden geregistreerd. Het kennissysteem wordt ook gebruikt om de procedures te beschrijven, zodat deze duidelijk zijn voor behandelaars en klanten.

Je kan de gegevens op verzoek verstrekken, bijvoorbeeld met de functionaliteit print/export in TOPdesk. Het corrigeren van onjuiste gegevens kan zelfs direct in TOPdesk. Voor een individu is het mogelijk om persoonlijke gegevens zo te overschrijven zodat het niet langer mogelijk is om dit individu te identificeren. Dit slaat op het 'recht om te vergeten'.

8 Creëer een veiligheidsincidentproces

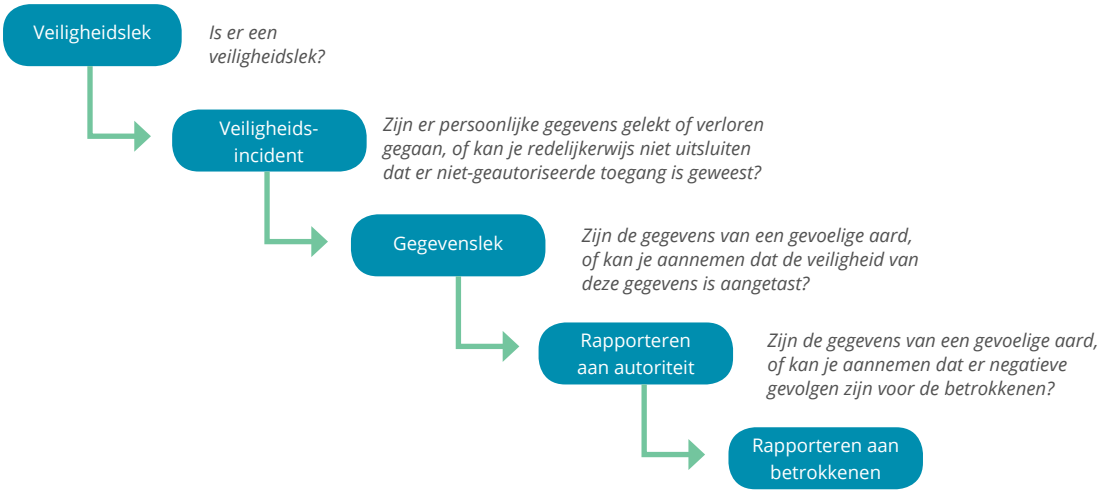
Voorkom stress bij een gegevenslek, zorg voor een veiligheidsincidentproces. In dit proces zorg je voor de juiste expertise om de impact van een incident te beoordelen, identificeer je acties die nodig zijn om een lek te dichten en (tijdelijke) maatregelen om de situatie op te lossen.

Een veiligheidsincidentproces zorgt ervoor dat je organisatie juist handelt bij een veiligheidslek. Neem contact op met TOPdesk Consultancy voor hulp bij het opstellen van een dergelijk proces.

Overweeg een specifiek e-mailadres met een TOPdesk mailimport en een selfserviceportal-formulier dat gebruikt kan worden voor het melden van veiligheidsincidenten. Met voorgedefinieerde categorieën of behandelaarsgroepen kan je behandelaars direct een e-mail sturen zodra ze een incident met hoge prioriteit krijgen toegewezen. Het helpt ook om voor klanten zichtbaar te maken hoe deze incidenten worden afgehandeld.

9 Rapporteer een gegevenslek

In sommige situaties moet je een veiligheidslek binnen 72 uur melden aan de juiste autoriteiten en/of de betrokkene(n). Maar te veel of onjuist rapporteren schaadt wellicht de reputatie van je organisatie. Het is slim om deze rapportageprocedure ook op te nemen in je veiligheidsincidentproces. Bepaal wie de rechten heeft om deze rapportage te doen. De procedures kunnen een dergelijke beslissingsstructuur hebben:



10

Zorg voor adequate (veiligheids)maatregelen

Iedere applicatie waar gevoelige gegevens in worden opgeslagen is onderhevig aan maatregelen. De applicatie en onderliggende infrastructuur, bijvoorbeeld besturingssystemen, databaseservers, netwerk etc., dienen moeten een beveiligde configuratie te hebben. Daarnaast moeten ze regelmatig worden geüpdatet om bekende kwetsbaarheden op te lossen. Bij TOPdesk On-premises is technische en procedurele kennis vereist om dit te regelen.

Bij TOPdesk SaaS kan je hiervoor rekenen op de expertise binnen TOPdesk. Door middel van onder andere continuous deployment, een gespecialiseerd team dat de omgevingen in de gaten houdt en beheerd en regelmatige veiligheidschecks door externe experts om te zorgen dat we altijd up-to-date zijn. Zo kan jij je volledig focussen op de klantervaring.

11

Rapporteer een gegevenslek aan de Verwerkingsverantwoordelijke

Gebruik je TOPdesk SaaS? Wij hebben een veiligheidsproces klaarstaan om te zorgen dat een lek snel wordt opgelost. Incidenten krijgen de hoogste prioriteit, zodat jij als verwerkingsverantwoordelijke binnen 8 werkuren na de ontdekking van het lek op de hoogte wordt gesteld. Daarnaast nemen we natuurlijk acties om de impact zo klein mogelijk te houden en vervelende situaties te vermijden.

Zo kan jouw organisatie voldoen aan de verplichtingen uit de GDPR en handelen volgens jullie eigen veiligheidsincidentprocessen.

12

Voer regelmatig veiligheidstesten en audits uit

We adviseren onze klanten om hun TOPdesk-systeem (en alle andere systemen met gevoelige informatie) periodiek te laten valideren. Je kan de beste experts hebben, maar een foutje is snel gemaakt. Bijvoorbeeld een standaard beheerderswachtwoord dat niet is gereset of een omgekeerde proxy die een oude versie draait. Hierdoor zijn jouw waardevolle gegevens in gevaar. Deze kwetsbaarheden zijn snel gevonden als je regelmatig tests laat uitvoeren door onafhankelijke experts.

Bij TOPdesk SaaS doen we dit voor jou. Toch blijven we onze klanten aanmoedigen om alles te dubbelchecken. We zijn erg dankbaar voor de vele veiligheidsrapporten die we ieder jaar ontvangen.

Valkuilen

Het is vaak niet ingewikkeld om een proces te creëren en te documenteren voor het beheren van gegevens. Het implementeren ervan wordt echter snel onderschat. Vooral het geven van instructies en het zorgen dat mensen bewust worden van hun eigen betrokkenheid bij het proces kan wat voeten in de aarde hebben.