FRUYTIER

Lawyers in Business

STAPPENPLAN

Hieronder volgt een stapsgewijs overzicht van de handelingen uit de Privacy Quick Scan die Fruytier Lawyers in Business samen met uw organisatie uitvoert. Hierdoor kunt u zich voorbereiden om zo efficiënt mogelijk compliant te zijn met de Algemene Verordening Gegevensbescherming (AVG).

De AVG wordt op 25 mei 2018 van kracht. Deze Algemene Verordening Gegevensbescherming (of General Data Protection Regulation, GDPR) vervangt de Europese privacyrichtlijn, en daarmee onze Wet bescherming persoonsgegevens (bij Uitvoeringswet AVG). Het bevat de regels voor verwerking van persoonsgegevens. Wat nieuw is, zijn bepaalde rechten voor betrokkenen en het feit dat de AVG verantwoording verlangt. Documenteer daarom wat uw organisatie doet met persoonsgegevens in het verwerkingsregister.

De quick scan zal er als volgt uit zien:

1. Introductie:

Fruytier Lawyers in Business introduceert haar Privacy Quick Scan met een uitleg van het privacy recht in vogelvlucht bij degene die in uw organisatie de compliance op het gebied van privacy in portefeuille heeft. Vervolgens inventariseren wij alle persoonsgegevensstromen binnen uw organisatie om te bezien met wie interviews zullen worden gehouden, denk bijvoorbeeld aan de afdeling HR, IT en marketing. Aan het eind van de introductie stemmen we een plan van aanpak af. Dit plan omvat onder meer afspraken omtrent de planning en interviews.

2. Interviews:

Fruytier Lawyers in Business voert interviews uit met de meest aangewezen afdelingen binnen uw organisatie om een beter inzicht te krijgen in de dagelijkse gegevensverwerkingen van uw organisatie.

3. Assesment:

Fruytier Lawyers in Business brengt uw privacy beleid in beeld door inventarisatie van bestaande documentatie. Wij beoordelen hoe het privacy beleid procedureel is geregeld en – belangrijker – hoe het onderwerp is geïntegreerd in uw organisatie.

4. Eindbespreking:

Fruytier Lawyers in Business voert een analyse uit op basis van de informatie die is verkregen in de voorgaande stappen en presenteert haar resultaten op een toegankelijke en eenvoudige manier. Wij tonen u aandachtspunten, dragen maatregelen aan om risico's weg te nemen en beantwoorden resterende privacy vragen.

STAPPENPLAN

1. Inventariseer welke categorieën van persoonsgegevens de organisatie verwerkt en voor welk doel deze worden gebruikt.
2. Beschrijf hoe en van welke categorie betrokkenen deze persoonsgegevens worden verzameld en aan wie deze worden verstrekt. In het geval de verwerking buiten de EER plaatsvindt, dienen daarvoor maatregelen te worden getroffen, zoals EU Model Clauses.
3. Beveiligingsbeleid: adequate technische en organisatorische beveiligingsmaatregelen gezien het soort gegevens en de te verwachten risico's; onderbouwing in verwerkingsregister waarbij u onderbouwt waarom uw beveiliging hieraan voldoet; rekening houden met onder meer de kosten en moeite.
4. Verwerking door derden dienen te worden geregeld in een verwerkingsovereenkomst.
5. Bij iedere verwerking moet een risico-inschatting worden gemaakt. Bij een hoog risico is een privacy impact assessment vereist.
6. Bepaal of een privacy officer vereist is. Dit is vereist voor overheidsinstanties, instellingen die op grote schaal bijzondere persoonsgegevens (zoals gezondheid, religie of etnische afkomst) verwerken en instellingen die mensen stelselmatig volgen of observeren (recherchebureaus, interesseprofielen als core business).
7. Informeer betrokkenen tijdig over de verwerking door middel van een duidelijke privacyverklaring.
8. Bepaal een beleid voor datalekken. Wie is intern verantwoordelijk voor melden?

PRIVACYBEGINSELEN

1. Inventariseer welke categorieën van persoonsgegevens de organisatie verwerkt en voor welk doel deze worden gebruikt.
2. Beschrijf hoe en van welke categorie betrokkenen deze persoonsgegevens worden verzameld en aan wie deze worden verstrekt. In het geval de verwerking buiten de EER plaatsvindt, dienen daarvoor maatregelen te worden getroffen, zoals EU Model Clauses.
3. Beveiligingsbeleid: adequate technische en organisatorische beveiligingsmaatregelen gezien het soort gegevens en de te verwachten risico's; onderbouwing in verwerkingsregister waarbij u onderbouwt waarom uw beveiliging hieraan voldoet; rekening houden met onder meer de kosten en moeite.
4. Verwerking door derden dienen te worden geregeld in een verwerkingsovereenkomst.
5. Bij iedere verwerking moet een risico-inschatting worden gemaakt. Bij een hoog risico is een privacy impact assessment vereist.
6. Bepaal of een privacy officer vereist is. Dit is vereist voor overheidsinstanties, instellingen die op grote schaal bijzondere persoonsgegevens (zoals gezondheid, religie of etnische afkomst) verwerken en instellingen die mensen stelselmatig volgen of observeren (recherchebureaus, interesseprofielen als core business).
7. Informeer betrokkenen tijdig over de verwerking door middel van een duidelijke privacyverklaring.
8. Bepaal een beleid voor datalekken. Wie is intern verantwoordelijk voor melden?

Fruytier Lawyers in Business – Kingsfordweg 99, 1043 GP Amsterdam – 020-5210130 – www.flib.nl