Hoe stelt u privacygegevens veilig?

INVESTEER IN GDPR-COMPLIANCE

SGS

Privacywetgeving

Is uw organisatie bekend met de eisen omtrent persoonsgegevens?

Uit een recent benchmark-onderzoek blijkt dat 59% van organisaties in 2019 voldeden aan een groot deel van de privacywetgeving. De grootste uitdagingen werden geïdentificeerd als gegevensbeveiliging, opleiding van werknemers en het bijhouden van de veranderende privacy-regelgeving.

PRIVACYGEGEVENS

WAAROM ZIJN ER REGELS OMTRENT PRIVACYGEGEVENS NODIG?

De aard van persoonlijke gegevens is de afgelopen twee decennia ingrijpend veranderd. Daarbij is de hoeveelheid digitale informatie die elke persoon produceert exponentieel gegroeid. Elke tweet, internetzoekactie, online aankoop of internet-cookie kan potentieel teruggekoppeld worden naar een individu en vormt daarmee een mogelijke bedreiging voor de privacy.

Privacy is daardoor een steeds grote zorg geworden voor organisaties. Zij hebben de verplichting om hun medewerkers en klanten te beschermen. Echter, de schaal en de verscheidenheid aan gegevens kunnen dit moeilijk maken. De omvang van het probleem wordt aangetoond door toename van gegevens die in databases bewaard worden. Geschat werd, dat de totale hoeveelheid gegevens in de wereld in 1986 ongeveer drie exabytes bedroeg. Tegen 2011 was dat naar schatting meer dan 300 exabytes. Sindsdien is dit aantal enorm gegroeid, vandaag wordt geschat dat alleen de VS al meer dan twee zettabytes aan gegevens heeft.

GENERAL DATA PROTECTION REGULATION (GDPR)

WELKE GEGEVENSRECHTEN ZIJN ER OPGENOMEN IN DE GDPR?

Per 25 mei 2018 is de GDPR verplicht in de EU. Dit met als doel: het recht van het individu, om zijn persoonlijke gegevens te beheren. In de GDPR zijn acht privacy rechten opgenomen, waaraan organisaties moeten voldoen:

1. **Recht op inzage -** Dit is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die u van hen verwerkt.
2. **Recht op vergetelheid -** Mensen hebben het recht om 'vergeten' te worden.
3. **Recht op rectificatie en aanvulling -** Het recht om de persoonsgegevens die u verwerkt te laten wijzigen.
4. **Het recht op dataportabiliteit -** Het recht om persoonsgegevens over te laten dragen aan een andere partij.
5. **Het recht op beperking van de verwerking -** Het recht om minder gegevens te laten verwerken.
6. **Het recht met betrekking tot geautomatiseerde besluitvorming en profilering -** oftewel: het recht op een menselijke blik bij besluiten.
7. **Het recht om bezwaar te maken tegen de gegevensverwerking -** een organisatie moet bepaalde activiteiten staken indien daarom wordt gevraagd.
8. **Het recht op duidelijke informatie -** Ten slotte hebben mensen recht op duidelijke informatie over wat u met hun persoonsgegevens doet.

bron: www.autoriteitpersoonsgegevens.nl

In België is informatie vindbaar via www.gegevensbeschermingsautoriteit.be.

RICHTLIJN 2016.679

HEEFT U INVLOED OP HET BOETEBEDRAG?

Bij een incident omtrent persoonsgegevens hebben ambtenaren (sinds de publicatie van de GDPR-wetgeving) de mogelijkheid om handhavingsacties uit te voeren die tot hoge boetes kunnen leiden. Echter, zullen de ambtenaren de maatregels die u heeft genomen, om datalekken voorkomen, meewegen in de beslissing van het maximale boetebedrag.

In de 'richtlijn voor de toepassing en vaststelling van administratieve boetes van de verordening 2016.679' zijn voorschriften opgenomen die uw organisatie kunnen helpen om maximumboetes te verminderen en eventueel te voorkomen.
U doet er als organisatie goed aan om de volgende vragen te beantwoorden:

- Wat is de aard, ernst en duur van de overtreding?
- Is er sprake van opzet/nalatigheid?
- Hoeveel individuen zijn slachtoffer geworden?
- Hoeveel moeite is gedaan om de schade voor individuen te beperken?
- Zijn er relevante eerdere overtredingen?
- Als er een overtreding heeft plaatsgevonden;
    - Hoe hebben we met de autoriteit samengewerkt, om de overtreding te repareren en de schadelijke effecten te beperken?
    - Op welke wijze hebben wij de overtreding gemeld bij de autoriteit?
    - Onder welke categorie valt de overtreding? Zo is een datalek van een telefoonnummer iets anders dan informatie over het ras, geloof of de medische toestand.

Organisaties die privacy-gegevens goed beheren, geven vertrouwen aan hun werknemers en klanten dat hun persoonlijke gegevens correct beschermd zijn.

GDPR-compliance

Is uw organisatie in staat gegevens-beveiliging te garanderen?

Het afgelopen jaar zijn er veel datalekken gemeld. Uit onderzoek blijkt dat organisaties die GDPR-compliance zijn hier minder problemen mee ervaren.

Mocht er toch onverwacht een datalek optreden, dan is het van belang dat uw organisatie weet hoe er gehandeld moet worden. Zo is het belangrijk dat uw organisatie kan aantonen dat de nodige maatregelen zijn getroffen om een mogelijk datalek te voorkomen. Daarnaast is het belangrijk dat iedereen in de organisatie weet wat ze moeten doen bij een datalek.

GDPR-COMPLIANCE ASSESSMENT

HOE STAAT UW ORGANISATIE ERVOOR?

Met een GDPR-compliance assessment kan onze auditor vaststellen:

- Hoe en waar de persoonsgegevens in de organisatie verwerkt worden.
- Hoe belanghebbenden geïnformeerd worden over het opslaan van de persoons-gegevens.
- Hoe veilig uw IT-systemen zijn.

De GDPR-compliance assessment geeft uw organisatie een duidelijk beeld van de huidige stand van zaken, omtrent privacywetgeving. Dit is het beginpunt voor het doorvoeren van verbetermaatregelen in uw organisatie.

Informatiebeveiliging

Kies voor ISO 27001-certificering om uw organisatie te beveiligen.

Er wordt veel gesproken over nieuwe datalekken en organisaties die gehackt zijn en waarbij belangrijke documenten zijn gegijzeld.

Heeft u er weleens bij stil gestaan wat de gevolgen zouden zijn voor uw organisatie? De gevolgen kunnen groot zijn, als er bijvoorbeeld door een hack of een datalek persoonsgegevens of bedrijfsgegevens in de verkeerde handen terechtkomen.

Als organisatie is het belangrijk dat u duidelijkheid krijgt op bepaalde zaken.

Weet u bijvoorbeeld het antwoord op de onderstaande vragen?

- Hoe zorgen wij ervoor dat we verantwoord en veilig omgaan met informatie?
- Hoe verminderen wij de kans op cyberaanvallen en ransomware?
- Wat kunnen de gevolgen zijn als vertrouwelijke gegevens in de verkeerde handen terechtkomen?

ISO 27001 is een managementsysteem voor informatiebeveiliging. Door het in kaart brengen van risico's kunt u informatie binnen uw organisatie beter beveiligen. Het implementeren van controlemaatregelen helpt om de kans op incidenten te verkleinen.

- U toont aan dat informatiebeveiliging op alle niveaus binnen uw organisatie belangrijk wordt gevonden.
- U geeft zekerheid naar klanten en werknemers dat u veilig omgaat met hun (privé)gegevens.
- U draagt bij aan het voldoen aan relevante wet- en regelgeving.
- U vermindert risico's en de kans op incidenten op gebied van gegevensbeveiliging.
- U brengt risico's in kaart en implementeert controlemaatregelen om deze risico's te beheren of uit te bannen.
- U beschermt zich met ISO/IEC 27001 tegen externe bedreigingen en minimaliseert de impact.

CONTACTINFORMATIE

www.sgs.be
www.sgs.nl

t +32 (0)3 545 48 48
t +31 (0)88 214 37 88

be.ssc.sales@sgs.com
nl.certificatie@sgs.com

www.sgs.com/linkedin

WHEN YOU NEED TO BE SURE