Digital Security
Progress. Protected.

ESET FOR MANUFACTURING
PRODUCTIE BEPAALT DE TOEKOMST

Digitale beveiliging voor productie

DIT ZIJN DE BELANGRIJKSTE WETGEVINGEN VOOR MANUFACTURING BEDRIJVEN:

Algemene Verordening Gegevensbescherming (AVG)

Deze Europese verordening legt eisen op aan de verwerking van persoonsgegevens en de bescherming van de privacy van individuen

NIS2

Wetgeving waarbij de aanbieder van essentiële diensten moet kunnen aantonen dat zij voldoen aan de organisatorische en technische eisen van NIS2

Wet bescherming bedrijfsgeheimen

Deze wet biedt bescherming aan bedrijfsgeheimen en vertrouwelijke bedrijfsinformatie

DIT IS HET BELANGRIJKSTE NORMENKADER IN MANUFACTURING:

ISO 27001

Dit is een internationale norm voor informatiebeveiliging. De norm bevat eisen voor het opzetten, implementeren, onderhouden en continu verbeteren van een Information Security Management System (ISMS).

NEN-EN-IEC 62443 (ICS)

Dit is een reeks normen voor de beveiliging van industriële controlesystemen (Industrial Control Systems, ICS), waaronder de beveiliging van productieprocessen en -apparatuur.

AVG

Een manufacturing bedrijf kan de Algemene Verordening Gegevensbescherming (AVG) naleven door te voldoen aan de verschillende verplichtingen die de AVG oplegt met betrekking tot de verwerking van persoonsgegevens. Hieronder volgen enkele stappen die een manufacturing bedrijf kan nemen om te voldoen aan de AVG:

1. **Bewustwording creëren:** Het is belangrijk om alle medewerkers van het manufacturing bedrijf bewust te maken van de AVG en de impact ervan op de organisatie. Dit kan bijvoorbeeld door middel van trainingen, workshops en communicatiecampagnes.
2. **Inventarisatie van persoonsgegevens:** Het manufacturing bedrijf moet in kaart brengen welke persoonsgegevens het verwerkt, waar deze gegevens worden opgeslagen en wie er toegang tot heeft. Deze inventarisatie kan helpen om risico's op het gebied van gegevensbescherming te identificeren.
3. **Uitvoeren van een Data Protection Impact Assessment (DPIA):** Dit is een instrument waarmee het manufacturing bedrijf de privacyrisico's van gegevensverwerking kan beoordelen en de benodigde maatregelen kan treffen.
4. **Implementeren van passende technische en organisatorische maatregelen:** Het manufacturing bedrijf moet zorgen voor passende beveiligingsmaatregelen om persoonsgegevens te beschermen, zoals versleuteling van gegevens, toegangscontroles en het regelmatig uitvoeren van back-ups.
5. **Privacy by design en privacy by default:** Het manufacturing bedrijf moet er rekening mee houden dat privacybescherming al in de ontwerpfase van producten, systemen en processen moet worden meegenomen. Daarnaast moet het bedrijf standaardinstellingen hanteren die de privacy van betrokkenen beschermen.
6. **Meldplicht datalekken:** Het manufacturing bedrijf moet een procedure hebben voor het melden van datalekken bij de Autoriteit Persoonsgegevens en betrokkenen als persoonsgegevens onbedoeld openbaar zijn geworden.
7. **Samenwerking met derden:** Als het manufacturing bedrijf samenwerkt met derden, bijvoorbeeld bij het uitbesteden van gegevensverwerking, dan moet het bedrijf afspraken maken over de bescherming van persoonsgegevens en de naleving van de AVG.

Door deze stappen te volgen kan een manufacturing bedrijf voldoen aan de verplichtingen van de AVG en de privacy van betrokkenen beschermen.

NIS2

Om te controleren of een maakindustrie bedrijf onder de NIS2 valt, moet het eerst bepalen of het als aanbieder van een essentiële dienst wordt beschouwd. Dit hangt af van de specifieke activiteiten en de impact die deze kunnen hebben op de continuïteit van belangrijke economische en maatschappelijke processen.

Als het bedrijf als aanbieder van een essentiële dienst wordt beschouwd, moet het voldoen aan de beveiligingseisen van de NIS2. De belangrijkste eisen hebben betrekking op:

- Risicobeheer: Het bedrijf moet risico's identificeren en beoordelen die verband houden met de beveiliging van zijn netwerk- en informatiesystemen, en passende maatregelen nemen om deze risico's te beperken.
- Incidentenbeheer: Het bedrijf moet maatregelen nemen om de impact van incidenten op de beveiliging van netwerk- en informatiesystemen te beperken, en moet dergelijke incidenten melden aan de bevoegde instanties.
- Continuïteitsbeheer: Het bedrijf moet plannen opstellen en uitvoeren om de continuïteit van zijn netwerk- en informatiesystemen te waarborgen.
- Compliance: Het bedrijf moet de naleving van de NIS2 evalueren en documenteren en deze informatie beschikbaar stellen aan de bevoegde instanties op verzoek.

Het is belangrijk om op te merken dat de eisen van de NIS-richtlijn 2 niet alleen betrekking hebben op technische maatregelen, maar ook op organisatorische en procedurele maatregelen. Zorginstellingen moeten daarom een alomvattende aanpak hanteren om aan de eisen van de NIS-richtlijn 2 te voldoen.

Wet bescherming bedrijfsgeheimen

Om te voldoen aan de Wet bescherming bedrijfsgeheimen kan een manufacturing bedrijf de volgende stappen nemen:

1. **Identificeren van bedrijfsgeheimen:** Het bedrijf moet de bedrijfsgeheimen die het wil beschermen, duidelijk identificeren en classificeren.
2. **Implementeren van passende beveiligingsmaatregelen:** Het bedrijf moet passende beveiligingsmaatregelen implementeren om de vertrouwelijkheid van de bedrijfsgeheimen te waarborgen. Dit omvat onder andere toegangscontrole, gegevensversleuteling en het implementeren van beleid en procedures voor informatiebeveiliging.
3. **Bewustmaking van medewerkers:** Medewerkers moeten worden geïnformeerd over de bedrijfsgeheimen en de beveiligingsmaatregelen die zijn geïmplementeerd om deze te beschermen. Het bedrijf kan trainingen en bewustmakingscampagnes organiseren om dit te bewerkstelligen.
4. **Ondertekenen van geheimhoudingsverklaringen:** Het bedrijf kan medewerkers en derde partijen die toegang hebben tot de bedrijfsgeheimen, laten ondertekenen voor een geheimhoudingsverklaring om extra bescherming te bieden.
5. **Monitoren van de naleving:** Het bedrijf moet regelmatig de naleving van de beveiligingsmaatregelen en het gebruik van bedrijfsgeheimen monitoren om te waarborgen dat de geheimhouding wordt gehandhaafd.

Het is belangrijk op te merken dat de Wet bescherming bedrijfsgeheimen voornamelijk gaat over de bescherming van informatie die niet openbaar is en waarvan de openbaarmaking schadelijk zou zijn voor de eigenaar van die informatie. Het is niet gericht op de bescherming van persoonsgegevens, hiervoor is de Algemene Verordening Gegevensbescherming (AVG) van toepassing.

ISO 27001/27002

Om te voldoen aan de ISO 27001/27002 normen kan een bedrijf uit de maakindustrie de volgende stappen nemen:

1. **Risicoanalyse:** voer een grondige risicoanalyse uit om de informatiebeveiligingsrisico's te identificeren en te evalueren.
2. **Beveiligingsbeleid:** stel een beleid op dat de basis vormt voor de implementatie van effectieve informatiebeveiligingsmaatregelen.
3. **Organisatorische maatregelen:** implementeer de nodige organisatorische maatregelen om de informatiebeveiliging te waarborgen, zoals het aanstellen van een security officer en het vaststellen van verantwoordelijkheden en bevoegdheden.
4. **Fysieke beveiligingsmaatregelen:** implementeer de nodige fysieke beveiligingsmaatregelen om de toegang tot gevoelige informatie te beperken, zoals toegangscontrolesystemen en bewaking van serverruimtes.
5. **Technische maatregelen:** implementeer de nodige technische beveiligingsmaatregelen om gegevens te beschermen tegen ongeoorloofde toegang, vernietiging of wijziging, zoals encryptie, firewalls en antivirussoftware.
6. **Monitoring en evaluatie:** voer regelmatig controles uit om te zorgen dat de genomen maatregelen effectief zijn en blijven, en om nieuwe risico's te identificeren en aan te pakken.
7. **Certificering:** laat een onafhankelijke certificeringsinstantie een audit uitvoeren om te bevestigen dat het bedrijf voldoet aan de eisen van de ISO 27001/27002 normen.

Het is aanbevolen om een ervaren informatiebeveiligingsprofessional in te schakelen om het bedrijf te begeleiden bij het implementeren van de benodigde maatregelen en om te helpen bij het behalen van de certificering.

NEN-EN-IEC 62443 (**ICS**)

De NEN-EN-IEC 62443 normenreeks is specifiek gericht op de cybersecurity van industriële automatiseringssystemen. Om als bedrijf uit de maakindustrie te voldoen aan deze normen, kan het de volgende stappen nemen:

1. Bepaal welke van de NEN-EN-IEC 62443 normen van toepassing zijn op de organisatie en de industriële automatiseringssystemen.
2. Voer een risicoanalyse uit om de risico's voor de cybersecurity van de industriële automatiseringssystemen te identificeren en te evalueren.
3. Implementeer maatregelen om de geïdentificeerde risico's te beheersen en te verminderen, met behulp van de best practices en richtlijnen die worden beschreven in de NEN-EN-IEC 62443 normenreeks.
4. Houd een veiligheidsbeheersysteem (VBS) bij om de veiligheid en beveiliging van de industriële automatiseringssystemen te monitoren, te meten en te verbeteren.
5. Zorg voor continue verbetering door regelmatig te evalueren of de maatregelen voldoen aan de normen en of ze effectief zijn bij het beheren van risico's voor de cybersecurity van de industriële automatiseringssystemen.

Het kan nuttig zijn om bij het implementeren van de NEN-EN-IEC 62443 normenreeks hulp in te roepen van gespecialiseerde cybersecurity-bedrijven of -consultants. Zij hebben de expertise en ervaring om bedrijven uit de maakindustrie te ondersteunen bij het naleven van deze normen.