

## THE TIMKEN COMPANY

### Wereldwijd beleid ten aanzien van gegevensprivacy

Over de hele wereld vereist gegevensprivacy, als nalevingsverplichting, steeds meer aandacht. De bezorgdheid die mensen over de privacy van hun persoonsgegevens hebben is groter geworden nu de technologie zich verder ontwikkeld heeft en de wereld steeds meer met elkaar verbonden geraakt is. Over de hele wereld hebben overheden op deze zorgen gereageerd met wetten die bedoeld zijn ter bescherming van persoonsgegevens en om de manieren waarop persoonsgegevens gebruikt kunnen worden te beperken. Timken zet zich ervoor in om deze zorgen te respecteren en deze wetten na te leven.

Dit beleid beschrijft de basisregels die alle medewerkers van Timken moeten volgen, ongeacht hun rol binnen het bedrijf. Medewerkers die zich vanwege hun functie directer bezighouden met het verzamelen, gebruiken en beschermen van persoonsgegevens of die verantwoordelijkheid dragen voor het beslissen hoe die informatie gebruikt en beschermd moet worden, hebben aanvullende verplichtingen die geïdentificeerd en uitgelegd worden in andere materialen die door het Global Data Privacy Office beschikbaar gesteld worden.

#### Wat is gegevensprivacy?

**Gegevensprivacy** – soms ook wel gegevensbescherming genoemd – is het nalevingsgebied dat ontworpen is voor de bescherming van **persoonsgegevens** over **individuen** tegen **ongepast gebruik** en tegen **ongeoorloofd verlies of openbaarmaking**.

**Persoonsgegevens** – soms ook wel persoonlijke gegevens genoemd – is elk stukje informatie, in welke vorm dan ook (elektronisch, papier, geluid of beeld), dat gebruikt kan worden, op zichzelf of met andere informatie, om *ofwel*

- een persoon te identificeren, zoals naam, burgerservicenummer, e-mailadres of foto, ofwel
- iets over een persoon te leren, registreren of beslissen, zoals werk- of opleidingshistorie, een communicatieverslag, informatie over financiële rekeningen of een strafblad.

**Privacy/bescherming.** Een voor de hand liggend doel van gegevensprivacywetten is het beschermen van persoonsgegevens tegen **ongeoorloofd verlies of openbaarmaking**. Deze wetten zijn echter ook ontworpen om persoonsgegevens te beschermen tegen **oneigenlijk gebruik**.

#### Wat zijn uw verplichtingen in het kader van dit beleid?

U speelt een belangrijke rol in het realiseren van Timkens toewijding aan gegevensprivacy. Door deze regels te volgen draagt u uw steentje bij:

**1. Begrijp de beginselen van gegevensprivacy en pas ze toe.** Het is belangrijk dat u de beginselen van gegevensprivacy begrijpt (deze worden later besproken), zelfs als het regelmatig en systematisch gebruik van persoonsgegevens niet onder uw werkzaamheden valt. We komen allemaal in contact met persoonsgegevens, zoals namen en contactgegevens van onze collega's of personen die tot onze klanten, leveranciers en andere zakenpartners behoren. Als u vragen hebt over het volgen van de beginselen en dit beleid moet u contact opnemen met uw leidinggevende, het Global Data Privacy Office of andere meldingshulpbronnen van Timken.

**2. Respecteer en bescherm de persoonsgegevens waar u mee te maken krijgt.** Deze algemene verplichtingen en beperkingen gelden voor alle medewerkers van Timken, ten aanzien van de persoonsgegevens waar ze in het kader van hun werkzaamheden mee te maken hebben.

#### DOEN:

- alle beleidsvoorschriften en toegangsregels ten aanzien van informatiebeveiliging kennen en naleven,

- redelijke maatregelen nemen om persoonsgegevens te beschermen tegen onopzettelijk of ongeoorloofd verlies, misbruik of openbaarmaking aan personen - zelfs andere medewerkers van Timken - die niet bevoegd zijn om de persoonsgegevens in te zien,
- periodieke controles uitvoeren ten aanzien van e-mails en documenten die u bewaart op uw computer en mobiele apparaten en op netwerkopslaglocaties die onder uw controle vallen en items met persoonsgegevens verwijderen die niet meer bewaard hoeven worden volgens geldende beleidsvoorschriften voor het bewaren van gegevens of voor onze zakelijke behoeften, en
- overtredingen van dit beleid melden zodra u daarvan op de hoogte bent.

#### **NIET DOEN:**

- de persoonsgegevens van anderen gebruiken buiten uw legitieme taken bij Timken,
- proberen om toegang te verkrijgen tot persoonsgegevens die niet noodzakelijk zijn voor het type en het toepassingsgebied van de aan u toegewezen taken, of toegang behouden tot persoonsgegevens die u onbedoeld verkregen hebt, of
- persoonsgegevens beschikbaar stellen aan een persoon of bedrijf, zowel binnen als buiten Timken, anders dan als onderdeel van uw taakverantwoordelijkheden en zoals geautoriseerd door de regels die gelden voor de zakelijke activiteit waarin de persoonsgegevens gebruikt zijn.

**3. Meld een inbreuk op persoonsgegevens.** U moet een vermeende inbreuk op persoonsgegevens zo snel mogelijk melden. Dit is extreem belangrijk aangezien veel wetten vereisen dat we bepaalde inbreuken op persoonsgegevens binnen een kort tijdsbestek moeten melden - onder sommige wetten moet dit binnen 72 uur plaatsvinden.

Een **inbreuk op persoonsgegevens** is een situatie die **heeft geleid** of die **lijkt te leiden tot** een inbreuk op de beveiliging die leidt tot de **onopzettelijke of onwettige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van, of toegang tot,** persoonsgegevens.

**4. Volg specifieke eisen die voor uw functie van toepassing zijn.** Sommige medewerkers moeten vanuit hun functie aanvullende maatregelen nemen die voortvloeien uit de gegevensprivacybeginselen en -wetten. Medewerkers van Timken die in een HR-functie werken zullen bijvoorbeeld regelmatig werken met de persoonsgegevens van Timken-medewerkers en moeten alle door hun organisatie voorgeschreven maatregelen voor het gebruik en de bescherming van die persoonsgegevens nemen. Deze medewerkers en hun leidinggevenden moeten er zeker van zijn dat deze specifieke maatregelen onderdeel worden van de zakelijke activiteit, gecommuniceerd worden aan alle medewerkers die bij de activiteit betrokken zijn en regelmatig op effectiviteit getest worden. Aanvullende hulpmiddelen en ondersteuning zijn beschikbaar via het Global Data Privacy Office.

#### **Wat zijn de beginselen van gegevensprivacy?**

De naleving van onze gegevensprivacy is opgebouwd rondom een reeks algemeen aanvaarde beginselen voor gegevensprivacy. Hoewel deze beginselen binnen verschillende organisaties op diverse wijzen vermeld en georganiseerd zijn, gebruikt Timken de volgende zeven beginselen. Deze beginselen worden nader toegelicht in de gids Beginselen van gegevensprivacy van Timken, die beschikbaar is op het onderdeel Timken Ethics and Compliance van TimkeNet.

**1. Rechtmatig, eerlijk en transparant.** Persoonsgegevens moeten op rechtmatige, eerlijke en transparante wijze verwerkt (gebruikt) worden ten aanzien van de gegevensbetrokkene.

**2. Doelbeperking.** Persoonsgegevens moeten verzameld worden voor gespecificeerde, expliciete en legitieme doeleinden en mogen niet verder verwerkt (gebruikt) worden op een wijze die onverenigbaar is met deze doeleinden.

- 3. Minimalisatie.** Persoonsgegevens moet adequaat, relevant en beperkt zijn tot wat nodig is ten aanzien van de doeleinden waarvoor de informatie verwerkt (gebruikt) wordt.
- 4. Nauwkeurigheid.** Persoonsgegevens moeten nauwkeurig zijn en, indien nodig, actueel gehouden worden; alle redelijke maatregelen moeten genomen worden om ervoor te zorgen dat persoonsgegevens die onjuist zijn, ten opzichte van de doelen waarvoor ze verwerkt (gebruikt) worden, zonder vertraging gewist of gecorrigeerd worden.
- 5. Retentiebeperking.** Persoonsgegevens mogen niet langer dan nodig is bewaard worden in een vorm die identificatie mogelijk maakt van gegevensbetrokkenen voor de doeleinden waarvoor de persoonsgegevens verwerkt (gebruikt) worden.
- 6. Integriteit en vertrouwelijkheid - Veiligheid.** Persoonsgegevens moeten verwerkt (gebruikt) worden op een wijze die voldoende beveiliging van de persoonsgegevens waarborgt, waaronder bescherming tegen ongeoorloofde of onrechtmatige verwerking (gebruik) en tegen onopzettelijk verlies, vernietiging of beschadiging, met behulp van passende technische of organisatorische maatregelen.
- 7. Verantwoording.** Een bedrijf dat persoonsgegevens verwerkt (gebruikt) moet verantwoordelijk zijn voor, en in staat zijn om de overige beginselen van gegevensprivacy te demonstreren.

#### **Hoe is dit beleid van toepassing?**

**Medewerkers.** Dit beleid is van toepassing op alle medewerkers van The Timken Company en haar wereldwijde dochterondernemingen voor de verzameling, verwerking, het gebruik, de verwerking, overdracht en opslag van persoonsgegevens van personen met wie Timken bij haar bedrijfsvoering in contact komt. Het beleid legt alle medewerkers en dochterondernemingen van Timken in alle landen gemeenschappelijke regels op, zelfs die landen of politieke onderverdelingen (zoals individuele staten binnen de VS) die geen strenge gegevensprivacywetten hebben. Sommige landen en politieke onderverdelingen hanteren strengere regels dan de norm en in die landen of politieke onderverdelingen moeten de medewerkers van Timken de strengere regel volgen.

**Leiderschap van dochterondernemingen.** Medewerkers die managementverantwoordelijkheid dragen voor de activiteiten van individuele dochterondernemingen van Timken of groepen gerelateerde dochterondernemingen moeten ervoor zorgen dat er voldoende en gekwalificeerd personeel en hulpmiddelen ingezet worden om een passend nalevingsniveau met de gegevensprivacybeginselen en -wetten te bereiken en dat elke bedrijfsactiviteit of -proces die persoonsgegevens gebruiken de specifieke maatregelen uitvoeren die door deze wetten vereist zijn, zoals aanbevolen door het Global Data Privacy Office. Dochterondernemingen van Timken mogen geen beleidsvoorschriften of praktijken aannemen die inconsistent met dit beleid zijn, behalve met goedkeuring van het Global Data Privacy Office, of zoals door de lokale wetgeving vereist is na kennisgeving aan en in overleg met het Global Data Privacy Office.

**Interpretatie en handhaving.** Dit beleid wordt uitgegeven door het Ethics and Compliance Office van Timken, die verantwoordelijk is voor de interpretatie ervan. Dit is een beleid met verplichtingen voor het wereldwijde personeelsbestand van Timken. Overtredingen van het beleid kunnen een medewerker onderwerpen aan disciplinaire maatregelen, tot en met de beëindiging van het dienstverband. Dit beleid kan alleen gewijzigd worden door het Ethics and Compliance Office, indien goedgekeurd door het uitvoerend management.

#### **Welke hulpmiddelen zijn er beschikbaar om bij de naleving te helpen?**

**Global Data Privacy Office.** Timken heeft binnen haar Ethics and Compliance Office een Global Data Privacy Office opgericht. Het Global Data Privacy Office zorgt voor toezicht, ondersteuning, kennis en coördinatie voor de leidinggevenden van verwerkingsactiviteiten en beheert bepaalde veelgebruikte hulpmiddelen en processen voor de naleving van gegevensprivacy. Het kantoor wordt geleid door een Global Data Privacy Compliance Lead (Global DPCL). De contactgegevens voor het Global Data Privacy Office zijn:

Timken Data Privacy Office

Postcode WHQ-02  
4500 Mount Pleasant St NW  
North Canton, OH 44720 U.S.A.  
[DataPrivacyOffice@timken.com](mailto:DataPrivacyOffice@timken.com)  
+1 234 262 2207  
866 846 5369 (Gratis in de VS)

**Meldingsbronnen voor ethiek en naleving.** U kunt bezorgdheden melden bij elk van deze meldingsbronnen voor ethiek en naleving:

- uw manager of leidinggevende
- uw HR-vertegenwoordiger
- een lid van het management
- de afdeling voor ethiek en naleving op [ethics@timken.com](mailto:ethics@timken.com)
- de Timken Helpline op [www.Timkenhelpline.com](http://www.Timkenhelpline.com)

**Gerefererde en gerelateerde beleidsvoorschriften**

- [Ethische bedrijfsnormen van Timken](#)
- [Wereldwijde beleidsvoorschriften voor informatiebeveiliging](#)
- HIPAA-privacyhandleiding – Beleidsvoorschriften en -procedures