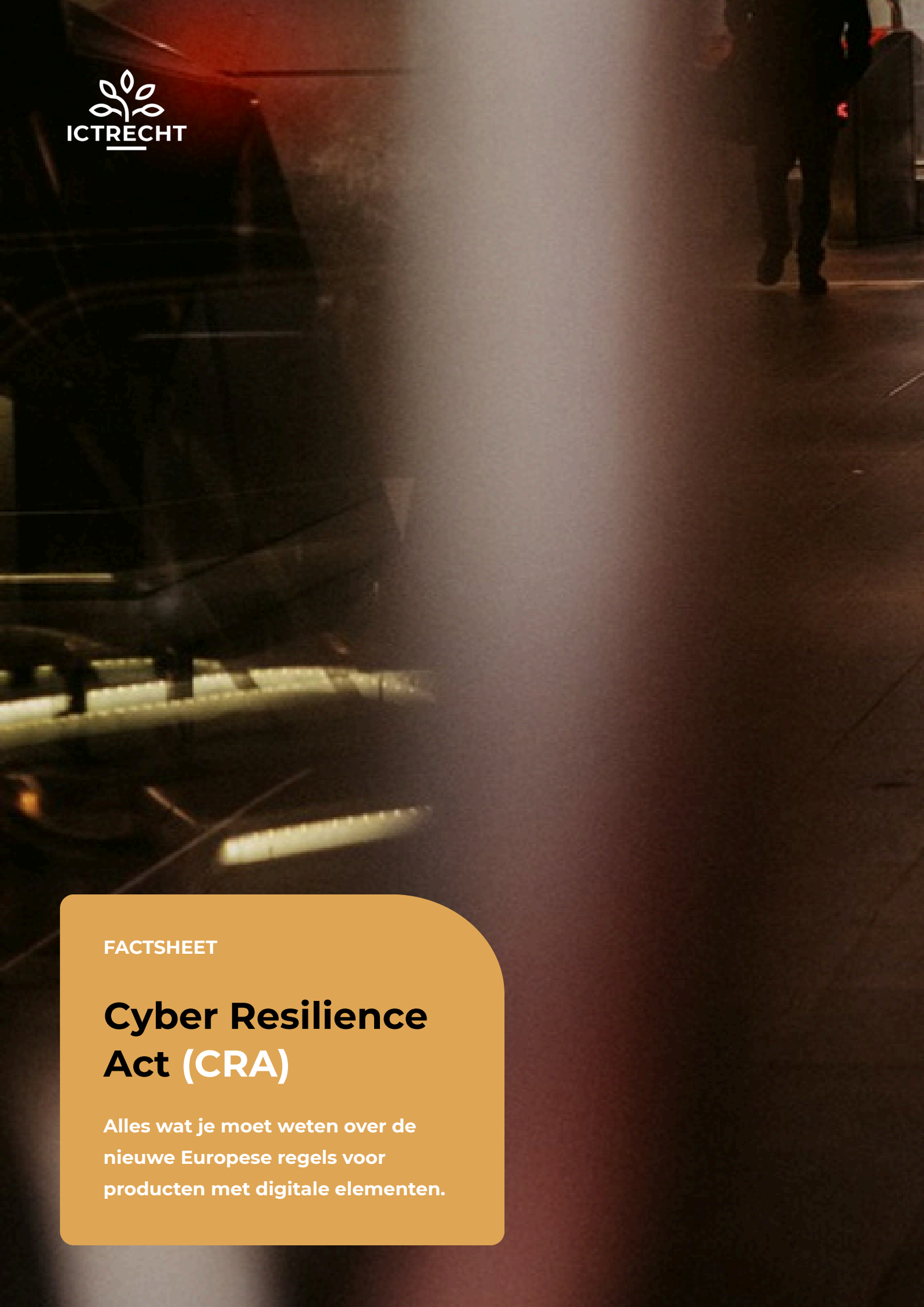


ICTRECHT

FACTSHEET

Cyber Resilience Act (CRA)

Alles wat je moet weten over de nieuwe Europese regels voor producten met digitale elementen.

Wat is de Cyber Resilience Act (CRA)?

De Cyber Resilience Act (Verordening (EU) 2024/2847) is een Europese verordening die cyberbeveiligingseisen stelt aan **producten met digitale elementen** die op de EU-markt worden aangeboden. De verordening is op 10 december 2024 in werking getreden.

De CRA is van toepassing op vrijwel alle hardware en software die verbonden is, of kan worden, aan het internet of een vergelijkbaar digitaal netwerk. Denk aan slimme apparaten zoals tv's, deurbellen en babyfoons, maar ook aan smartphones, smartwatches, laptops, tablets, e-readers én alle software die daarop geïnstalleerd is of kan worden.

Vier pijlers van de CRA

Veiligere producten

minder kwetsbaarheden bij marktintroductie.

Levenscyclus-benadering

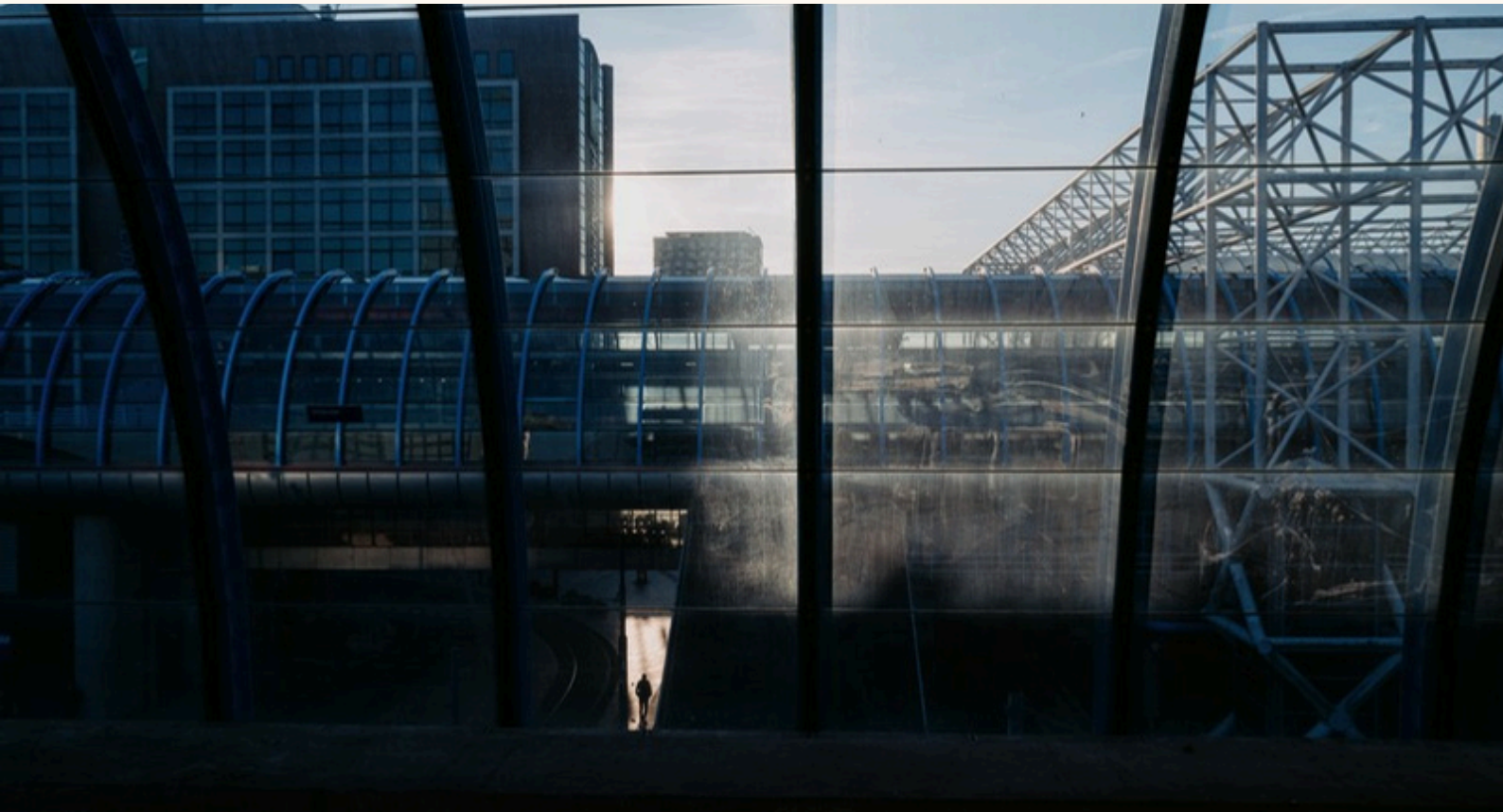
beveiliging gedurende de gehele ondersteuningsperiode of verwachte levensduur.

Transparantie

gebruikers krijgen inzicht in cyberbeveiligingskenmerken en ondersteuningsperiode.

Incident response

actief uitgebuite kwetsbaarheden en ernstige incidenten worden gemeld aan toezichthouders en (geraakte) gebruikers.



Waarom is de CRA er, en vanaf wanneer gaat het in?

Centrale gedachte: alles wat aan het internet (of een vergelijkbaar digitaal netwerk) verbonden is, loopt risico om gehackt te worden. De CRA verplicht organisaties om passende maatregelen te treffen: kwetsbaarheden voorkomen, in de gaten houden of er toch digitale inbrekers (criminelen of zelfs vijandige statelijke actoren) binnen zijn gekomen, en snel handelen als dat het geval is. Hoe belangrijker of gevoeliger het product en hoe groter de mogelijke schade, hoe zwaarder de maatregelen moeten zijn.

Datum	Wat gaat in?
11 juni 2026	Aanmelding conformiteitsbeoordelingsinstanties (hoofdstuk IV)
11 september 2026	Meldplicht kwetsbaarheden en incidenten (art. 14)
11 december 2027	Volledige toepassing (conformiteitsbeoordeling, CE-markering, technische documentatie)

Let op: de meldplicht treedt **15 maanden eerder** in werking dan de meeste andere verplichtingen, en geldt óók voor producten die al eerder op de markt zijn gebracht. Bepaal dus vóór 11 september 2026 of jouw organisatie onder de CRA en de meldplicht valt.

Wat betekent het concreet?

Productcategoieën

De CRA kent productcategorieën met eisen aan beveiliging en aan de manier waarop conformiteit moet worden aangetoond, passend bij de risico's: **standaard, belangrijk klasse I of II, en kritiek.** De categorie bepaalt de conformiteitsroute (interne controle, externe partij of aangemelde instantie, of certificaat met ten minste zekerheidsniveau "substantieel"). Voor kritieke producten (Bijlage IV) kan een verplichte Europese cyberbeveiligingscertificering worden voorgeschreven via een gedelegeerde handeling.

Vijf rollen onder de CRA

- **Fabrikant:** ontwikkelt (of laat ontwikkelen) producten die onder eigen naam of merk in de handel worden gebracht, of wijzigt producten ingrijpend.
- **Gemachtigde vertegenwoordiger:** partij die fabrikant die buiten de EU is gevestigd vertegewoordigd**.**
- **Importeur:** brengt producten van buiten de EU in de handel.
- **Distributeur:** biedt producten aan zonder eigenschappen te beïnvloeden.
- **Open-source software steward:** beheert opensourcesoftware zonder zelf fabrikant te zijn.

Meldplicht: 3-fasenmodel (art. 14)

Fabrikanten moeten actief uitgebuite kwetsbaarheden en ernstige incidenten melden aan het bevoegde CSIRT en aan ENISA, via het Single Reporting Platform (SRP) dat ENISA opzet (art. 16).

Fase	Termijn	Inhoud
Vroegtijdige waarschuwing	Binnen 24 uur na kennisname	Indicatie van getroffen lidstaten. Incident: minimaal of het vermoedelijk door onwettige of kwaadwillige handelingen is veroorzaakt.
Kwetsbaarheids- of incidentmelding	Binnen 72 uur na kennisname	Algemene informatie over product, aard van uitbuiting of incident, eerste beoordeling, genomen risicobeperkende maatregelen, corrigerende maatregelen voor gebruikers.
Eindverslag	Kwetsbaarheid: binnen 14 dagen nadat corrigerende maatregel beschikbaar is. Incident: binnen 1 maand na incidentmelding.	Beschrijving, ernst, gevolgen, oorzaak, kwaadwillige actor, beveiligingsupdate of details corrigerende maatregelen.

Gebruikers informeren

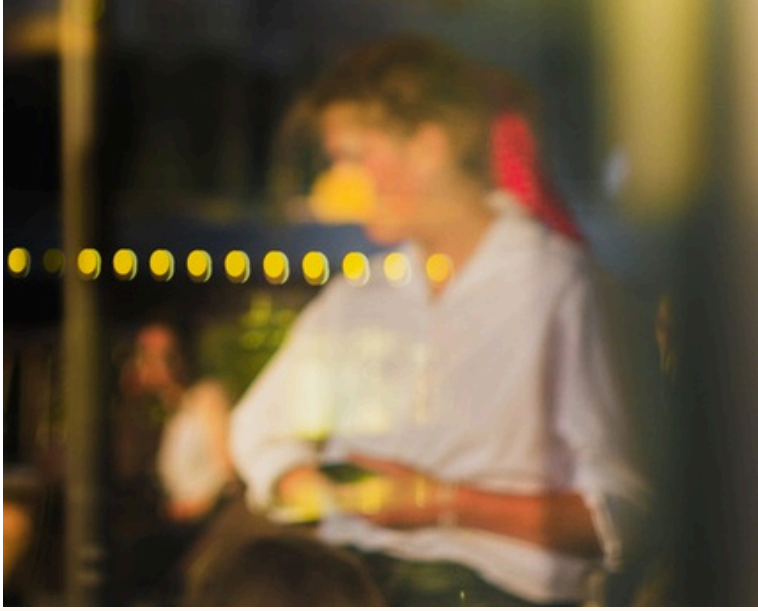
naast de melding aan CSIRT/ENISA moet de fabrikant getroffen gebruikers (en indien passend alle gebruikers) op de hoogte stellen van de kwetsbaarheid of het incident en van risicobeperkende maatregelen, bij voorkeur in een gestructureerd, machineleesbaar formaat zoals een direct uit te voeren security-update (art. 14 lid 8). Daarbij moet worden vermeden dat de informatie door (andere) kwaadwillenden misbruikt kan worden.

Vrijwillige melding

fabrikanten en andere natuurlijke of rechtspersonen kunnen ook vrijwillig kwetsbaarheden, cyberdreigingen en incidenten melden aan CSIRTs. Meldt iemand anders dan de fabrikant, dan informeert het CSIRT de fabrikant.

conformiteitsbeoordelingsinstanties (vanaf 11 juni 2026)

Op grond van art. 71 lid 2 zijn de bepalingen over aanmelding van conformiteitsbeoordelingsinstanties (hoofdstuk IV, art. 35 t/m 51, in het Engels "notified bodies") van toepassing vanaf 11 juni 2026. Dit is met name relevant voor **belangrijke en kritieke producten:** fabrikanten moeten tijdig een aangemelde instantie benaderen voor de conformiteitsbeoordeling en CE-markering.



Sancties

Overtreding	Maximale boete
Schending essentiële eisen (Bijlage I) of art. 13/14	€15 mln of 2,5% wereldwijde jaaromzet
Schending overige verplichtingen (o.a. art. 18-23, 28, 30-33, 39, 41, 47, 49, 53)	€10 mln of 2% wereldwijde jaaromzet
Onjuiste of misleidende info aan aangemelde instanties of markttoezicht	€5 mln of 1% wereldwijde jaaromzet

Micro- en kleine ondernemingen krijgen geen boete voor overschrijding van de 24-uurstermijn (art. 64 lid 10).

Hoe bereid ik me voor?

- Voer een CRA-toepasselijkheidsbeoordeling (applicability assessment) en rolkwalificatie uit voor het hele productportfolio.
- Classificeer alle producten (standaard, belangrijk klasse I of II, kritiek).
- Voer een CRA-volwassenheidsbeoordeling (maturity assessment) of gap-analyse uit op de essentiële cyberbeveiligingsvereisten (Bijlage I) en de andere toepasselijke verplichtingen.
- Stel een roadmap op om de juiste conformiteitsbeoordeling uit te voeren en CE-markering(en) aan te brengen vóór 11 december 2027. Denk aan implementatiestappen zoals:
    - Richt als fabrikant vóór 11 september 2026 het meldproces in voor actief uitgebuite kwetsbaarheden en ernstige incidenten.
    - Integreer een gedocumenteerde cyberbeveiligingsrisicobeoordeling in het productontwikkelingsproces, verwerk de resultaten in de technische documentatie (Bijlage VII) en betrek het beoogde doel én redelijkerwijs voorzienbaar gebruik en misbruik.
    - Zorg voor gebruikersinstructies en transparantie.
    - Verwerk CRA-eisen in contracten met leveranciers en afnemers.

Hulp nodig?

Wij kunnen ondersteuning bieden bij alle bovenstaande acties. Neem contact op om de mogelijkheden te bespreken.

ICTRECHT

Benieuwd wat wij voor jouw organisatie kunnen betekenen?

Bezoek onze website voor meer informatie.

www.ictrecht.nl/cra
020 - 663 1941