creditsafe

GDPR Klantenbriefing 2018

Hoe Creditsafe GDPR gebruikt om betere zaken te doen

creditsafe

Inleiding

Wat is GDPR?

GDPR (General Data Protection Regulation - Algemene Verordening inzake Gegevensbescherming) - biedt een stevig pakket regels voor het verzamelen, opslaan en verwerken van persoonlijke informatie en treedt in werking op 25 mei 2018. De GDPR is eerder een verordening dan een richtlijn, wat betekent dat het als één enkele wetgevingshandeling van toepassing is in alle Europese lidstaten.

Waarom GDPR?

Aangezien bedrijven enorme hoeveelheden persoonlijke gegevens over consumenten verzamelen, van gedragsanalyses tot persoonlijke kenmerken, is persoonlijke privacy en bescherming ervan een belangrijk onderwerp en aandachtspunt geworden. Veel bedrijven hebben uitgebreide bedrijfsmodellen ontwikkeld die worden gestuurd door het verhandelen van informatie in ruil voor toegang tot diensten. Hoewel dit enorme kansen biedt, beschikken individuen weinig controle over waar hun gegevens voor worden gebruikt, hoe ze worden opgeslagen en kan het hen als gevolg daarvan blootstellen aan diefstal, fraude en andere misbruiken. Door de maatregelen te versterken, streeft de EU ernaar het vertrouwen te verbeteren en de algemene bedreiging voor individuen te verminderen.

Het introduceren van GDPR weerspiegelt de vooruitgang in technologie en gegevens van de afgelopen twee decennia. Door de maatregelen te versterken, streeft de EU ernaar het vertrouwen te verbeteren en de algehele bedreiging voor individuen te verminderen. De GDPR streeft ernaar de wetgeving inzake gegevensbescherming in heel Europa op elkaar af te stemmen, gelijke voorwaarden te scheppen en, nog belangrijker, het voor bedrijven eenvoudiger te maken het naleven ervan te begrijpen en te beheren.

Op wie is GDPR van toepassing?

GDPR heeft gevolgen voor alle organisaties die persoonlijke gegevens over EU-burgers bewaren. Het maakt niet uit waar in de wereld de gegevens worden opgeslagen.

GDPR verruimt de *definitie van persoonsgegevens* om zo alles te behelzen dat kan worden gebruikt om een persoon direct of indirect te identificeren. Dit omvat een breed spectrum aan gegevens van bijvoorbeeld namen, foto's, e-mailadressen, bankgegevens en berichten op sociale netwerksites tot medische informatie of IP-adressen. De nieuwe verordening beoogt de bescherming van deze gegevens, ongeacht of de archivering automatisch of handmatig is, op papier of elektronisch.

Bij het beoordelen van gegevens van B2B versus B2C en wat wel of niet onder de bevoegdheid van GDPR valt, lijkt de scheidingslijn tussen persoonlijke en zakelijke gegevens niet altijd duidelijk gedefinieerd. Persoonsgegevens van bedrijven zonder rechtspersoonlijkheid zoals eenmanszaken of vennootschappen of directiegegevens van geregistreerde bedrijven moeten volgens de definitie van GDPR bijvoorbeeld worden beschouwd als persoonlijk identificeerbare gegevens.

creditsafe

Wat zijn de belangrijkste actoren in GDPR?

Organisaties zullen rekenschap verschuldigd zijn aan de toezichthoudende autoriteiten voor gegevensbescherming. Hoewel de aansprakelijkheid geen nieuwe vereiste is, vereist GDPR van alle organisaties dat ze de naleving van alle geldende aspecten van GDPR registreren en documenteren. De verordening verleent individuen meer rechten met betrekking tot hun gegevens, waaronder meer controle en zichtbaarheid over hoe hun persoonlijke gegevens worden gebruikt, en het recht om die informatie op verzoek te laten verwijderen of verplaatsen.

Gegevenssubject

Gegevenssubjecten zijn de particuliere personen (EU-burgers) over wie gegevens worden verzameld en verwerkt, bijvoorbeeld individuen, werknemers, bestuurders, aandeelhouders, bedrijfseigenaars, etc. GDPR biedt gegevenssubjecten meer rechten met betrekking tot de gegevens die door bedrijven worden verwerkt en beheerd. Dit wordt meestal beschreven als *empowerment* van de gegevenssubjecten

Gegevensbeheerder

De gegevensbeheerder bepaalt de doelen en middelen voor het verwerken van persoonlijke gegevens. Ze bepalen de manier waarop persoonlijke gegevens worden verwerkt, wat inhoudt dat ze zeggenschap hebben over het "waarom" en "hoe" van alle gegevensverwerking. Gegevensbeheerders worden niet van hun verplichtingen ontheven wanneer er een gegevensverwerker bij betrokken is - de GDPR stelt verdere verplichtingen om ervoor te zorgen dat uw contracten met gegevensverwerkers voldoen aan de GDPR. Creditsafe is een gegevensbeheerder.

Gegevensverwerker

De gegevensverwerker is verantwoordelijk voor het verwerken van persoonsgegevens in opdracht van een gegevensbeheerder. De GDPR stelt specifieke wettelijke verplichtingen; gegevensverwerkers zijn bijvoorbeeld verplicht om registers bij te houden over persoonlijke gegevens en verwerkingsactiviteiten. Gegevensverwerkers zijn wettelijk aansprakelijk als ze verantwoordelijk zijn voor een overtreding.

Autoriteit op Gegevensbescherming

AG's zijn onafhankelijke overheidsinstanties die via onderzoeksbevoegdheden en corrigerende maatregelen toezicht houden op de toepassing van de wet inzake gegevensbescherming. Ze bieden deskundig advies over kwesties i.v.m. gegevensbescherming en behandelen klachten die zijn ingediend tegen schendingen van de Algemene Verordening op Gegevensbescherming en de relevante nationale wetgeving. In elke Europese lidstaat is er een aanwezig.

Functionaris voor gegevensbescherming

De primaire rol van de functionaris voor gegevensbescherming (FGB) is er voor te zorgen dat de organisatie de persoonlijke gegevens van personeel, klanten, leveranciers of andere personen verwerkt in overeenstemming met de geldende regels op gegevensbescherming. De geldende Verordening op Gegevensbescherming (Verordening (EG) 45/2001) verplicht elk van de Europese instellingen en organen om een FGB aan te wijzen. Creditsafe heeft een FGB aangesteld op groepsniveau en beschikt over mensen die de functie van FGB uitvoeren waar dergelijke benoeming adequaat is volgens de reglementering of handelspraktijken.

creditsafe

De essentiële gebieden van GDPR

1. **Aansprakelijkheid**

   Gegevensbeheerders moeten kunnen aantonen dat de organisaties de GDPR naleven. Het is echter de aansprakelijkheid van zowel de verwerkers als de beheerders om ervoor te zorgen dat de juiste procedures worden gevolgd.

2. **Transparantie**

   Organisaties moeten open en transparant zijn over de reden waarom zij persoonsgegevens verzamelen en hun bedoeling ermee. Dit betekent dat ze vooraf aan het gegevenssubject moeten uitleggen waarvoor ze de gegevens wensen te gebruiken en dat ze er toestemming voor dienen te verkrijgen.

3. **Verwerken van persoonsgegevens**

   Persoonsgegevens kunnen alleen worden verzameld voor specifieke, expliciete en legitieme doeleinden en mogen niet worden verwerkt in een andere hoedanigheid die niet aan deze doeleinden voldoet. Gegevens die rechtmatig zijn verzameld voor één welbepaald doel, kunnen bijgevolg niet voor een ander doel worden gebruikt tenzij ze toestemming van de betrokkene verkrijgen of een legitiem doel hebben om dit te doen.

4. **Recht op toegang**

   Gegevenssubjecten hebben het recht om binnen 30 dagen na een verzoek toegang te krijgen tot hun persoonsgegevens. Organisaties dragen de verantwoordelijkheid om ervoor te zorgen dat onjuiste gegevens worden bijgewerkt of gewist; gegevenssubjecten het recht geven om persoonlijke informatie over hen te controleren en te wijzigen.

5. **Recht om vergeten te worden**

   Gegevenssubjecten hebben ook het recht om te vragen dat hun persoonlijke gegevens worden verwijderd, op voorwaarde dat er geen legitieme redenen zijn om deze te bewaren.

6. **Standaard Gegevensbescherming (Effectbeoordeling inzake Privacy)**

   GDPR roept op te evalueren hoeveel en hoe lang we persoonlijke gegevens bewaren. Een Effectbeoordeling inzake Privacy kan vereist zijn in omstandigheden met een hoog risico. Het bepaalt ook dat de organisatie bij het verzamelen van persoonlijke gegevens over een individu geen gegevens mag verzamelen die overschrijden wat nodig is voor het beoogde doel.

7. **Boetes voor impact op de privacy of schending van rechten**
   Er kunnen boetes van maximaal 4% van de jaarlijkse omzet of 20 miljoen euro, al naargelang welk bedrag het hoogste is, worden opgelegd voor inbreuken op GDPR.

8. **Melden van inbreuken**
   In het geval van een data-inbreuk die een impact zou kunnen hebben op het individu of schade zou kunnen veroorzaken, moet de gegevensbeheerder de toezichthoudende autoriteit hiervan op de hoogte brengen binnen 72 uur na het ontdekken van het lek.

Impact van GDPR op de informatiediensten van Creditsafe.

Creditsafe heeft als bedrijf de verplichting om gegevens over bedrijven en hun verloop in de geschiedenis te verzamelen om zo de kredietwaardigheid van ondernemingen te beoordelen. Creditsafe biedt zijn klanten gegevens aan waarmee zij financiële beslissingen kunnen nemen en bedrijfsrisico's kunnen beheren. Persoonlijke identificeerbare informatie (PII) die wordt beheerd door Creditsafe gaat alleen over personen die rechtstreeks verbonden zijn met een bedrijfseenheid1.

Creditsafe is actief in een business to business (B2B) omgeving. Creditsafe beschikt over PII van individuen, hetzij als onderdeel van een organisatie zoals een bestuurder of als een eenmanszaak, waarbij het individu het bedrijf is. Creditsafe beoordeelt alleen het vermogen van de bedrijfsentiteit om bedrijfsactiviteiten uit te voeren en blijven uit te voeren en contracten na te komen op basis van prestaties in het heden en in het verleden. Het type en de kwaliteit van gegevens die aan klanten worden verstrekt, zullen als zodanig niet veranderen na de introductie van GDPR.

Gegevens die door Creditsafe werden verzameld maar ongeschikt werden bevonden voor gebruik of niet beschikken over de juiste toestemming, worden gewist.

Legitieme belang in het leveren van informatiediensten

GDPR Artikel 6: F staat de verwerking toe ten behoeve van de legitieme belangen die worden nagestreefd door de gegevensbeheerder of een derde. Verder wordt bepaald dat gegevensbeheerders persoonsgegevens kunnen verwerken zonder toestemming indien er een echte en legitieme reden voor is. Dit kan commerciële voordelen inhouden, behalve wanneer dergelijke belangen geannuleerd worden door de belangen of fundamentele rechten en vrijheden van het gegevenssubject en die bescherming van persoonsgegevens vereisen.

Het is het legitieme belang van Creditsafe om het de bedrijven te makkelijker te maken om financiële beslissingen te nemen gebaseerd op risico zodat onze klanten betere zakelijke en economische beslissingen kunnen nemen. We handhaven als zodanig ook het legitieme belang om bedrijven bewust te maken van deze mogelijkheid.

Beheerder-beheerderrelatie

Bij Creditsafe kunnen klanten kiezen uit vele verschillende productaanbiedingen. Er is over de hele lijn een wisselende mate van flexibiliteit in de manier waarop Creditsafe dienstverlening en informatie verstrekt en selecteerd. Creditsafe gebruikt zijn eigen database voor het leveren van diensten en kan beslissen waarvoor deze gegevens verder nog worden gebruikt. Creditsafe zal met andere woorden optreden als een gegevensbeheerder. Deze positie wordt behandeld in de standaard contractuele bepalingen.

Creditsafe treedt op als gegevensbeheerder telkens als er diensten worden verleend aan de klant: Creditsafe gebruikt zijn eigen gegevens en kan zelf beslissen wat er mee te doen; er is flexibiliteit om te beslissen hoe de taak moet worden uitgevoerd, welke gegevens er moeten worden opgenomen en wat belangrijk is voor het samenstellen

1 De bedrijven van Creditsafe in Zweden en Noorwegen verzamelen en verwerken ook gegevens over consumenten volgens de bepalingen van de wetgeving op kredietreferentie.

van het rapport. Dit betekent dat Creditsafe volledig verantwoordelijk is voor alle gegevensverwerking en ervoor moet zorgen alleen persoonsgegevens te delen wanneer dit wettelijk is toegestaan.

Samengevat geven alle gegevens, verstrekt door Creditsafe en vervat in de producten en dienstverlening, aanleiding tot een controller-naar-controllerrelatie met onze klanten waarvoor er *geen verwerkingsclausules vereist zijn*. Ongeacht de 'controller-naar-controller'relatie met klanten, neemt Creditsafe de clausules voor gegevensbescherming op in de standaard algemene voorwaarden voor klanten.

Als beheerder moet Creditsafe ervoor zorgen dat het alleen persoonlijke gegevens deelt indien wettig toegelaten. Daarom stelt Creditsafe in de algemene voorwaarden het kader voor het delen van persoonlijke gegevens en een bevestiging van de klant dat ze een wettige basis moeten hebben om onze diensten te gebruiken. De algemene voorwaarden van Creditsafe bevat een lijst met redenen waarom een klant onze producten kan gebruiken.

Sommige specifieke informatiediensten zijn:

Invoer voor zoekactie

Volgens de niet-bindende zienswijze van de DPA zijn/waren zoektermen niet relevant. Het bedrijf dat eigenaar was van de database was eigenlijk een databeheerder van de database. Wwanneer het door middel van een rapport informatie naar de klant stuurde, zou de klant databeheerder worden van dat rapport. Daarom is het in eerste instantie een kwestie van al dan niet rechtmatig kunnen delen van informatie - de zoektermen zijn een vals spoor.

Gegevens zuiveren / toevoegen en betalingsgegevens uitwisselen

Creditsafe 'regelt' welke correcties (dienen) worden aangebracht in deze gegevens en welke aanvullende informatie / gegevens moeten worden toegevoegd als onderdeel van de dienstverlening. Creditsafe heeft de flexibiliteit om te beslissen hoe de taak moet worden uitgevoerd - We zijn zeer waarschijnlijk een 'beheerder' van die gegevens.

Kunnen onze klanten onze informatie gebruiken?

Ja, al onze gegevens en producten zijn afgestemd op de vereisten van onze klanten. We gebruiken zowel gegevens (conform de toestemming of legitiem belang) en verstrekken gegevens aan klanten op dezelfde basis.

De klant is verantwoordelijk voor het bepalen van de wettelijke basis voor het verwerken van persoonsgegevens, die zijn verkregen door gebruik te maken van de informatiediensten van Creditsafe, en om de wetgeving inzake gegevensbescherming in verband met dergelijke gegevens na te leven. De klant moet ook erkennen dat toegang tot persoonsgegevens door gebruik van de informatiediensten van Creditsafe alleen is toegestaan indien de klant een wettelijke basis heeft om dit te doen.

Dit betekent bijvoorbeeld dat de klant de informatiediensten van Creditsafe alleen mag gebruiken voor het controleren van kredietwaardigheid, prospectie, direct marketing, verificatie 'ken uw klant', compliance, gegevensverificatie en -uitbreidingen, andere wettelijke due diligence-doeleinden of alle andere zakelijke activiteiten met een legitiem belang ten opzichte van GDPR

Hoe Creditsafe afgestemd is op GDPR

Creditsafe heeft GDPR volledig zakelijk benaderd en alle bedrijfsprocessen en gegevensprocessen geëvalueerd om ervoor te zorgen dat deze aansluiten bij de legitieme belangen van onze onderneming om klanten te helpen bij het nemen van financiële beslissingen op basis van feitelijke risicobeoordelingen. Dit proces heeft ons in staat gesteld om de bronnen en het gebruik van al onze gegevens te onderzoeken, om ervoor te zorgen dat we onze klanten de diensten kunnen aanbieden die ze willen, terwijl we er tegelijkertijd voor zorgen dat geen van onze praktijken schade of nadeel berokkent aan individuen geïdentificeerd in onze gegevensbestanden.

Onze databronnen en opslag begrijpen (datamapping)

We gaan bij alle stadia van gegevensbewaring na wat we doen met de gegevens, hoe we de gegevens beschermen en hoe we ervoor zorgen dat we geen inbreuk plegen op de rechten van het gegevenssubject. Dit houdt onder meer in dat persoonsgegevens uitsluitend worden verkregen voor welbepaalde en wettige doeleinden en verder niet zullen worden verwerkt op enigerlei wijze die onverenigbaar is met dat doel of die doeleinden.

Inzicht in het gebruik van gegevens voor de specifieke doeleinden waarvoor de gegevens werden verzameld

Rechtmatig belang, administratie behandeling, toestemming, waarborg dat gegevens adequaat, relevant en niet overdreven zijn met betrekking tot het doel. Creditsafe evalueert systematisch haar gegevens om legitiem belang te controleren.

Bescherming van de rechten van het individu

Creditsafe heeft processen geïmplementeerd om alle rechten van individuen te behandelen, inclusief Verzoek om Toegang vanwege Gegevenssubject (SAR), Recht om te Worden Vergeten (R2BF), Gegevenscorrectie, Wijzigen van Gegeven Toestemming, Gegevens verplaatsen naar een ander platform voor individueel gebruik.

Gegevensintegriteit en transparantie

De Data Vault-processen van Creditsafe beheren en stempelen de gegevens, wat de volledige traceerbaarheid van alle Creditsafe-gegevens garandeert. Door duidelijk te laten zien waar de gegevens vandaan komen en eventuele wijzigingen die zijn doorgevoerd met de reden voor de wijziging.

Het implementeren van passende technische en organisatorische maatregelen om gegevens te beschermen

Tegen ongeoorloofde of onwettige verwerking van persoonsgegevens en tegen onopzettelijk verlies of vernietiging van of schade aan persoonsgegevens. Creditsafe implementeert technologieën die ons in de eerste plaats in staat zullen stellen om gevoelige Persoonlijke Identificeerbare Informatie (PII) te identificeren en vervolgens te taggen, waardoor alle gegevens worden beschermd. Dit garandeert dat de gegevens niet worden misbruikt of verwijderd buiten het Creditsafe-netwerk door ongeoorloofde acties.

- Firewalls - Alle toegangspoorten/uitgangen van het netwerk worden beschermd door een firewall.
- DMZ's - Goed gedefinieerd voor openbare servers, met interne netwerksegmentatie die wordt gebruikt om gevoelige bronnen verder te isoleren.
- HIDS / NIDS - Ingeschakeld op de belangrijkste knelpunten op het netwerk.
- SIEM - Netwerken gecontroleerd door SIEM, met registratie en analyse van beveiligingsincidenten, geautomatiseerde waarschuwingen en ingestelde alarmen.
- Antivirus - Alle compatibele eindpunten worden beschermd door antivirussoftware, met automatische updates via een updateserver en internet.
- Netwerk/Host scannen - Regelmatig scannen op kwetsbare configuraties.
- Regelmatige grondige testen, testen van webtoepassingen en scannen op beveiligingsproblemen - Ingesteld programma voor risicobeheer en beveiligingsproblemen om de output te beheren.
- Preventie van Gegevensverlies: Creditsafe heeft controles geïmplementeerd om gegevens te beschermen tegen het verlaten van het netwerk tenzij toegelaten, zowel via netwerken als via externe mediabronnen

Het implementeren van geschikte controles

Om te voorkomen dat gegevens worden overgedragen naar een land of gebied buiten de Europese Economische Ruimte, tenzij dat land of gebied zorgt voor een passend niveau van bescherming van de rechten en vrijheden van gegevenssubjecten met betrekking tot de verwerking van persoonsgegevens.

Klaar om te reageren

Creditsafe heeft processen geïmplementeerd waarmee snel en efficiënt kan worden gereageerd op elk vermoedelijk incident, inclusief inbreuken die van invloed kunnen zijn op PII-gegevens. Creditsafe staat klaar met duidelijke en beknopte communicatieplannen voor klanten, subjectgegevens en regelgevende instanties ingeval van een incident dat kan leiden tot het treffen van een persoon.

Privacy door Ontwerp

Creditsafe realiseert zich dat GDPR geen alleenstaande gebeurtenis in de geschiedenis is en in plaats daarvan wordt het gebruikt als richtlijn voor onze toekomstige bedrijfsmodellen waarbij privacy door ontwerp wordt toegepast in onze interacties met individuen en in onze bedrijfsstrategie, zodat alle toekomstige zakelijke beslissingen en ontwikkelingen rekening houden met de impact op het individu vooraleer we verder gaan

creditsafe

Veelgestelde vragen

Is Creditsafe volledig conform met GDPR?

Creditsafe is bezig met een volledig GDPR-programma om te verzekeren dat onze activiteiten en dienstverlening volledig in lijn zijn met de regelgeving.

Creditsafe heeft als bedrijf de verplichting om gegevens over bedrijven en hun verloop in de geschiedenis te verzamelen om zo onderzoek te kunnen doen en hun klanten gegevens te verstrekken om financiële beslissingen te nemen en bedrijfsrisico's te beheren. PII die wordt afgehandeld door Creditsafe is alleen van die personen die direct verbonden zijn met een bedrijfsentiteit.

Creditsafe is actief in een business to business (B2B) omgeving. Wanneer we beschikken over PII van individuen, hetzij als deel van een organisatie zoals een directeur of als een eenmanszaak waarbij het individu de onderneming is, beoordelen we alleen het vermogen van de bedrijfsentiteit om zaken te doen en te blijven doen en om contracten te vervullen op basis van prestaties uit het verleden. Het type en de kwaliteit van gegevens die aan klanten worden verstrekt, zullen als zodanig niet veranderen na de introductie van GDPR. Gegevens die door Creditsafe werden verzameld maar ongeschikt werden bevonden voor gebruik of niet beschikken over de juiste toestemming, worden gewist.

Welke beveiligingssoftware en -codering heeft u om alle gegevens te beschermen die Creditsafe heeft verzameld en / of verwerkt?

- Creditsafe is ISO27001-gecertificeerd, gereguleerd door de FCA en geregistreerd als een gegevensbeheerder bij het kantoor van de Britse Information Commissioner.
- Creditsafe werkt via een Tier3 + UK-datacenter dat wordt gecontroleerd volgens de normen ISO9001, ISO14001, ISO27001, ISAE3402, SSAE16 en PCI DSS.
- Uitgebreide fysieke beveiliging van datacenters, waaronder wanden ontworpen in 6 lagen, 24/7 patrouilles op het terrein, omheiningen van militair niveau, digitale tripwires, meerdere IR CCTV-torens en gebouwd volgens Californische aardbevingsnormen.
- Beveiligingsopties van Creditsafe omvatten:
- Firewalls - Alle toegangspoorten/uitgangen van het netwerk worden beschermd door een firewall.
- DMZ's - Goed gedefinieerd voor openbare servers, met interne netwerksegmentatie die wordt gebruikt om gevoelige bronnen verder te isoleren.
- HIDS / NIDS - Ingeschakeld op de belangrijkste knelpunten op het netwerk.
- SIEM - Netwerken gecontroleerd door SIEM, met registratie en analyse van beveiligingsincidenten, geautomatiseerde waarschuwingen en ingestelde alarmen.
- Antivirus - Alle compatibele eindpunten worden beschermd door antivirussoftware, met automatische updates via een updateserver en internet.
- Data encryptie
- Netwerk/Host scannen - Regelmatig scannen op kwetsbare configuraties.
- Regelmatige grondige testen, testen van webtoepassingen en scannen op beveiligingsproblemen - Ingesteld programma voor risicobeheer en beveiligingsproblemen om de output te beheren.
- Bata Backup-gegevens worden met tussenpozen van 5 minuten gekopieerd van de productieomgeving van Creditsafe naar een specifieke omgeving voor bedrijfscontinuïteit. Het platform is gedimensioneerd en

geconfigureerd voor gebruik in hoge mate van beschikbaarheid waardoor geautomatiseerde fail-over van servers mogelijk is.

Marketinggegevens van Creditsafe

Hoe bereidt Creditsafe de marketinggegevens voor GDPR voor?

Creditsafe is bezig met een volledig GDPR-programma om ervoor te zorgen dat alle gegevens worden verzameld en gebruikt met de juiste toestemming, ongeacht of het gaat over toestemming of legitiem belang. Het gebruik van gegevens wordt volledig in kaart gebracht doorheen het hele bedrijf en onderworpen aan strenge risicobeoordelingen en effectbeoordeling op gebied van persoonlijke levenssfeer.

Welke toestemming vraagt Creditsafe van de bedrijven?

Toestemming verkregen door Creditsafe is relevant voor het gebruik van de gegevens die op dat moment worden verzameld, d.w.z. toestemming voor gebruik, toestemming voor het in de handel brengen, toestemming voor bellen en toestemming voor het bijwerken van bestanden voor toekomstig contact.

Wanneer er in bepaalde situaties geen toestemming beschikbaar ism staat GDPR Artikel 6: F de verwerking toe ten behoeve van de legitieme belangen die worden nagestreefd door de gegevensbeheerder of een derde. Het is het legitieme belang van Creditsafe om het de bedrijven eenvoudiger te maken om financiële beslissingen te nemen gebaseerd op risico zodat onze klanten betere zakelijke en economische beslissingen kunnen nemen. Daarom behouden we ook het legitieme belang om bedrijven bewust te maken van deze mogelijkheid, ook wanneer ze nieuwe zakelijke kansen nastreven.

Waar worden alle gegevens die we gebruiken gehost?

Alle gegevens van Creditsafe worden in het Verenigd Koninkrijk of binnen de EER opgeslagen op beveiligde servers die volledig zijn beveiligd voor herstel ingeval van ramp.