pension consultants
& actuaries

Hoe beschermen wij de gegevens van onze klanten?

Maart 2023

Gegevensbescherming door Bell Pension Consultants & Actuaries B.V.

Dit document beschrijft de maatregelen die Bell Pension Consultants & Actuaris B.V. (hierna: Bell) heeft genomen ter bescherming van klantgegevens en ter voldoening aan wet- en regelgeving inzake gegevensbescherming. Het beschrijft ook de stappen die Bell heeft ondernomen om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Wij zullen dit document regelmatig bijwerken op basis van aanpassingen in onze procedures en ons beleid. De laatste update dateert van maart 2023.

pension consultants
& actuaries

Inhoud

1 AVG

1.1 Hoe is de AVG geïmplementeerd binnen Bell?

1.2 Hoe zorgt Bell ervoor dat haar partners en werknemers handelen conform de AVG?

2 Governance

2.1 Hoe is de bescherming van gegevens door Bell gestructureerd en wie binnen Bell is daar verantwoordelijk voor?

3 Beschermingsbeleid

3.1 Welk beleid inzake bescherming van gegevens heeft Bell?

4 Werknemers

4.1 Doet Bell een screening van nieuwe werknemers voorafgaand aan indiensttreding?

4.2 Bevat de arbeidsovereenkomst bij Bell een geheimhoudingsverklaring ter bescherming van klantgegevens?

5 Training

5.1 Krijgen werknemers van Bell trainingen ter verhoging van besef van goede gegevensbescherming?

6 Waar worden klantgegevens door Bell bewaard?

6.1 Worden gegevens van Bell opgeslagen buiten Nederland? Welke maatregelen zijn genomen om te voorkomen dat gegevens van Bell terechtkomen buiten de EER?

7 Gegevensverwerking

7.1 Hoe zorgt Bell ervoor dat klantgegevens worden beperkt tot hetgeen noodzakelijk is voor het overeengekomen doel?

7.2 Gebruikt Bell haar klantgegevens ook voor andere doelen dan de doelen waarvoor deze oorspronkelijk zijn verkregen?

7.3 Welke extra maatregelen heeft Bell getroffen ter bescherming van extra gevoelige persoonsgegevens?

7.4 Gebruikt Bell verwerkersovereenkomsten en welke afspraken worden in dat geval gemaakt met de verwerkingsverantwoordelijke?

7.5 Maakt Bell gebruik van subverwerking en welke afspraken worden in dat geval gemaakt met de subverwerker?

8 Gegevenslekken en inbreuken op beveiliging

8.1 Heeft Bell ooit een gegevenslek moeten rapporteren aan de Autoriteit Persoonsgegevens? Is Bell ooit betrokken geweest bij een onderzoek van de Autoriteit Persoonsgegevens?

8.2 Hoe worden gegevenslekken en inbreuken op de beveiliging binnen Bell afgehandeld?

8.3 Welke procedures zijn getroffen om zeker te zijn dat klanten worden geïnformeerd over gegevenslekken?

9 Verzoeken van Betrokkenen

9.1 Welke procedure kent Bell met betrekking tot verzoeken van Betrokkenen inzake hun Persoonsgegevens?

10 Bedrijfscontinuïteit

10.1 Wat heeft Bell gedaan ter voorkoming van een significant veiligheidsprobleem?

11 Back-up en vernietiging van gegevens

11.1 Hoe vindt de back-up van klantgegevens plaats? Kan Bell de gegevens van een specifieke klant terug halen in het geval van

een systeemstoring en/of verlies van gegevens?

11.2 Welk beleid hanteert Bell met betrekking tot het bewaren van gegevens?

11.3 Hoe gaat Bell om met verzoeken om klantgegevens te corrigeren of te vernietigen?

12 Vernietiging

12.1 Hoe vernietigt Bell klantgegevens op papier?

12.2 Hoe vernietigt Bell mobiele gegevensdragers en hoe stelt zij servers en apparaten die klantgegevens bevatten buiten werking?

13 Audit en certificering

13.1 Beschikt Bell over gegevensbescherming certificaten?

13.2 Wordt het beleid ten aanzien van gegevensbescherming intern of extern beoordeeld?

14 Toegang tot IT-systemen en toegang op afstand

14.1 Heeft Bell een procedure om ongepaste of niet-geautoriseerde IT-activiteit te ontdekken en te managen?

14.2 Hoe garandeert Bell dat haar werknemers (inclusief inleenkrachten) de juiste toegangsrechten tot de IT-systemen hebben?

14.3 Welke oplossingen gebruikt Bell om haar werknemers toegang op afstand tot haar netwerk te bieden?

15 Beveiliging

15.1 Welke beveiliging wordt toegepast om laptops en netwerk van Bell te beveiligen?

15.2 Voert Bell toegangscontroles op haar netwerk en systemen uit, en zo ja, hoe vaak?

15.3 Gebruikt Bell draadloze netwerken? Hoe zijn deze beveiligd?

15.4 Welke technische en organisatorische maatregelen zijn door Bell getroffen om klantgegevens binnen haar kantoor te beveiligen?

15.5 Hoe worden partijen die toegang hebben tot systemen met klantgegevens of deze managen, gecontroleerd?

16 Versleuteling

16.1 Hoe worden klantgegevens naar externe partijen verzonden en wordt daarbij gebruikt gemaakt van versleuteling?

16.2 Hoe worden mobiele gegevens versleuteld?

1 AVG

1.1 Hoe is de AVG geïmplementeerd binnen Bell?

Binnen Bell is een persoon aangewezen, de Security & Privacy Officer (hierna: de SPO) die verantwoordelijk is voor het bevorderen dat Bell AVG-compliant is. De SPO toetst regelmatig interne procedures en processen waarbij sprake is van verwerking van Persoonsgegevens beoordeelt en waar nodig acties ter verbetering initieert. De SPO zorgt ervoor dat Bell niet alleen nu maar ook in de toekomst AVG-compliant is.

1.2 Hoe zorgt Bell ervoor dat haar partners en werknemers handelen conform de AVG?

Gegevensbescherming is een regelmatig terugkerend onderwerp op de agenda voor regulier teamoverleg binnen Bell. Partners en werknemers zijn verplicht om de jaarlijkse interne training "Security & Privacy" bij te wonen, waarin (vernieuwde) procedures worden besproken. Alle werknemers van Bell zijn verplicht een AVG-protocol te ondertekenen, waarin een werknemer verklaart bekend te zijn met de te volgen procedures voor gegevensbescherming en de verantwoordelijkheden en plichten in het kader van de AVG na te leven.

2 Governance

2.1 Hoe is bescherming van gegevens door Bell gestructureerd en wie binnen Bell is daar verantwoordelijk voor?

Bell hanteert een gegevensbeschermingsprotocol op basis waarvan klantgegevens op passende en veilige manier kunnen worden bewaard en verwerkt. De SPO is verantwoordelijk voor het gegevensbeschermingsbeleid. Binnen het reguliere teamoverleg wordt, indien daar aanleiding toe is, het beleid en de uitvoering daarvan besproken en worden, indien nodig, verbeteringen in het beleid en de controle op de uitvoering daarvan doorgevoerd.

3 Beschermingsbeleid

3.1 Welk beleid inzake bescherming van gegevens heeft Bell?

Bell heeft diverse beleidsmaatregelen genomen. Zo kent zij richtlijnen voor bijvoorbeeld het gebruik van wachtwoorden, (technische) hulpmiddelen zoals mobiele telefoons en laptops, hanteert zij een clean desk beleid met betrekking tot vertrouwelijke gegevens, en heeft zij een protocol voor het geval een (vermoeden van) een gegevenslek wordt ontdekt.

4 Werknemers

4.1 Doet Bell een screening van nieuwe werknemers voorafgaand aan indiensttreding?

Bell doet een screening van kandidaat-werknemers. Deze screening bevat onder andere: adresverificatie, arbeidsverleden, opleiding, professionele kwalificaties en het opvragen van een Verklaring Omtrent Gedrag. Ook nemen we contact op met vorige werkgevers.

4.2 Bevat de arbeidsovereenkomst bij Bell een geheimhoudingsverklaring ter bescherming van klantgegevens?

Ja.

5 . Training

5.1 Krijgen werknemers van Bell trainingen ter verhoging van besef van goede gegevensbescherming?

Werknemers krijgen bij indiensttreding een training op het gebied van gegevensbescherming. Alle werknemers zijn verplicht om de jaarlijkse interne training “Security & Privacy” te volgen. Het beschermingsbeleid van Bell is gedocumenteerd en beschikbaar voor al haar werknemers. Het beleid en de uitvoering daarvan wordt , indien daar aanleiding toe is, besproken tijdens het reguliere teamoverleg.

6 Waar worden klantgegevens door Bell bewaard?

6.1 Worden gegevens van Bell opgeslagen buiten Nederland? Welke maatregelen zijn genomen om te voorkomen dat gegevens van Bell terechtkomen buiten de EEA?

Digitale klantgegevens worden opgeslagen in de Microsoft cloud (alleen in de Europese datacentra), waarbij gebruik wordt gemaakt van Sharepoint / Microsoft 365. Dit platform voldoet aan algemeen geaccepteerde (technische) standaarden op het gebied van informatiebeveiliging en cybersecurity. Gegevens kunnen alleen benaderd worden met de juiste autorisaties.
De backup-faciliteiten zijn gevestigd in een Nederlands datacentrum.

Incidenteel wordt voor het draaien van speciale tooling, waarbij geen vertrouwelijke gegevens van toepassing zijn, nog gebruikt van de Private cloud van de externe IT-beheerder. Deze in Nederland gevestigde cloud is, mits daartoe geautoriseerd, alleen via een beveiligd Virtual Private Network (VPN) te benaderen.

7 Gegevensverwerking

7.1 Hoe zorgt Bell er voor dat klantgegevens worden beperkt tot hetgeen noodzakelijk is voor het overeengekomen doel?

Bij aanvang van iedere opdracht komen wij met onze klant doel en aard van onze werkzaamheden overeen en de gegevens die wij daarvoor nodig hebben.

7.2 Gebruikt Bell haar klantgegevens ook voor andere doelen dan de doelen waarvoor deze oorspronkelijk zijn verkregen?

Er kunnen specifieke situaties voorkomen waarin wij gegevens voor andere doelen gebruiken dan oorspronkelijk is overeengekomen met de klant. Dit zal over het algemeen zijn om onze dienstverlening aan de klanten te verbeteren. In zo'n situatie zullen wij alleen volledig geanonimiseerde gegevens of niet-persoonsgegevens gebruiken. Mocht dit niet mogelijk zijn, dan zullen we eerst expliciet aanvullende toestemming vragen bij de klant. Er kunnen ook speciale situaties zijn waarin wij uit hoofde van wet- en regelgeving ten behoeve van een toezichthouder Persoonsgegevens moeten verwerken. Indien zo'n verzoek van een toezichthouder ons bereikt, zullen wij de klant hierover onverwijld informeren.

7.3 Welke extra maatregelen heeft Bell getroffen ter bescherming van extra gevoelige Persoonsgegevens?

Gezien de aard van de werkzaamheden verwerkt Bell geen extra gevoelige Persoonsgegevens als bedoeld in artikel 9 AVG noch gegevens van strafrechtelijke aard als bedoeld in artikel 10 AVG. Extra maatregelen zijn daarom niet nodig.

7.4 Gebruikt Bell verwerkersovereenkomsten en welke afspraken worden in dat geval gemaakt met de verwerkingsverantwoordelijke?

Indien alleen sprake is van het adviseren over collectieve pensioenregelingen en/of bemiddelen bij pensioen-, arbeidsongeschiktheid- en verzuimverzekeringen is een verwerkingsovereenkomst niet nodig. Bell is in deze gevallen geen "Verwerker" in de zin van de wet, maar "Verwerkingsverantwoordelijke". Om de advies- of bemiddelingsopdracht te kunnen uitvoeren hebben wij Persoonsgegevens nodig, maar het verwerken daarvan is geen doel op zich. Wij besluiten zelfstandig welke gegevens nodig zijn en op welke wijze deze in het kader van de opdracht worden gebruikt. Uiteraard zijn wij als verwerkingsverantwoordelijke verplicht zorgvuldig om te gaan met Persoonsgegevens. In dit document beschrijven wij hoe hier door ons invulling aan wordt geven.
Als sprake is van een bijzondere situatie waarin voor het verwerken van Persoonsgegevens wel een verwerkersovereenkomst nodig is, dan zullen wij die

in overleg met de opdrachtgever opstellen, als onderdeel van de opdrachtovereenkomst.

7.5 Maakt Bell gebruik van subverwerking en welke afspraken worden in dat geval gemaakt met de subverwerker?

Bell maakt in beginsel geen gebruik van subverwerking. Mocht Bell toch gebruik willen maken van subverwerking dan zullen wij een verklaring eisen van de subverwerker dat zij haar plichten uit hoofde van de AVG aantoonbaar zal nakomen. Indien wij een subverwerker inschakelen dan zullen wij onze opdrachtgever hiervoor eerst om toestemming vragen.

8 Gegevenslekken en inbreuken op beveiliging

8.1 Heeft Bell ooit een gegevenslek moeten rapporteren aan de Autoriteit Persoonsgegevens? Is Bell ooit betrokken geweest bij een onderzoek van de Autoriteit Persoonsgegevens?

Bell heeft nooit een gegevenslek moeten rapporteren aan de Autoriteit Persoonsgegevens. Bell is ook nooit betrokken geweest bij een onderzoek van de Autoriteit Persoonsgegevens.

8.2 Hoe worden gegevenslekken en inbreuken op beveiliging binnen Bell afgehandeld?

Bell heeft een inbreukprocedure op grond waarvan de SPO moet worden geïnformeerd. Deze coördineert vervolgens escalatie, onderzoek en herstel. Bell heeft via haar externe IT-beheerder diverse waarschuwingsmechanismen in gebruik om incidenten te ontdekken. Betrokken klantenteams worden direct gewaarschuwd ingeval van kritische gebeurtenissen (bijvoorbeeld een malware aanval). Bell heeft via haar exteren IT-beheerder ook een gemanaged Inbraak Detectie Systeem ter beveiliging van web-gebaseerde toepassingen. Bell ontvangt bericht van dreigingen die zijn opgetreden. Alle apparaten van Bell zijn voorzien van Endpoint Protectie. Deze software zorgt ervoor dat malware automatisch wordt gedetecteerd en verwijderd. Tevens biedt deze software de mogelijkheid om bestanden na bijvoorbeeld een ransomware-aanval te herstellen. Ook wordt indien een gegevenslek en/of inbreuk op de beveiliging heeft plaatsgevonden door de externe IT-beheerder een forensisch rapport opgesteld om aan te tonen wat er is gebeurd, en waar een eventueel gegevenslek heeft plaatsgevonden.

8.3 Welke procedures zijn getroffen om zeker te zijn dat klanten worden geïnformeerd over gegevenslekken?

Indien zich een gegevenslek voordoet, waarbij gegevens van een klant betrokken kunnen zijn, zal deze hierover worden geïnformeerd en zal nader onderzoek naar het incident worden gedaan. Dit is onderdeel van de inbreukprocedure (zie 8.2).

9 Verzoeken van Betrokkenen

9.1 Welke procedure kent Bell met betrekking tot verzoeken van Betrokkenen inzake Persoonsgegevens?

Bell heeft in een schriftelijke instructie vastgelegd hoe om te gaan met verzoeken van Betrokkenen inzake Persoonsgegevens (zoals het recht op inzage, correctie, overdracht en vernietiging). Dit document wordt – in overleg met de SPO – regelmatig geactualiseerd om ervoor te zorgen dat het blijft voldoen aan de eisen die de AVG daaraan stelt.

10 Bedrijfscontinuïteit

10.1 Wat heeft Bell gedaan ter voorkoming van een significant veiligheidsprobleem?

De belangrijkste maatregel die Bell heeft getroffen is het extern opslaan van alle klantgegevens in de Microsoft cloud (zie 6.1). Daardoor kan Bell, op basis van "Conditional Access" vanaf elke plek buiten kantoor inloggen op haar systeem en blijven functioneren met zo min mogelijk verstoring voor klanten.

11 Back-up en vernietiging van gegevens

11.1 Hoe vindt de back-up van klantgegevens plaats? Kan Bell de gegevens van een specifieke klant terug halen in het geval van een systeemstoring en/of verlies van gegevens?

Voor alle gegevens wordt in de Microsoft cloud de algemeen geaccepteerde retentieperiode van 30 dagen aangehouden. Alle gegevens die binnen deze termijn zijn opgeslagen kunnen worden teruggehaald.

11.2 Welk beleid hanteert Bell met betrekking tot het bewaren van gegevens?

Bell bewaart gegevens zo lang dat noodzakelijk is om te voldoen aan wet- en regelgeving en onze professionele verplichtingen.

11.3 Hoe gaat Bell om met verzoeken om klantgegevens te corrigeren of te vernietigen?

Verzoeken van klanten om gegevens te corrigeren zullen wij voor zover mogelijk honoreren. Verzoeken van klanten om gegevens te vernietigen zullen wij honoreren voor zover dit in overeenstemming is met ons beleid dan wel de met de klant gemaakte speciale afspraken.

12 Vernietiging

12.1 Hoe vernietigt Bell klantgegevens op papier?

Papieren klantgegevens die vernietigd moeten worden, worden gedeponeerd in een afgesloten papierbak, die periodiek wordt geleegd door een gecertificeerd papiervernietigingsbedrijf.

12.2 Hoe vernietigt Bell mobiele gegevensdragers en hoe stelt zij servers en apparaten die klantgegevens bevatten buiten werking?

Bell maakt gebruik van gecertificeerde bedrijven om alle gegevens te vernietigen van computerhardware die uit bedrijf wordt genomen (inclusief disk, servers, werkstations, back-up tapes). Mobiele telefoons worden gereset naar de fabrieksinstellingen, waarbij alle gegevens gewist worden, voordat deze in gebruik worden genomen door een ander dan wel definitief buiten gebruik wordt gesteld.

13 Audit en certificering

13.1 Beschikt Bell over gegevensbescherming certificaten?

Bell beschikt niet over gegevensbescherming certificaten.

13.2 Wordt het beleid inzake bescherming van gegevens intern of extern beoordeeld?

Het beleid inzake bescherming van gegevens wordt intern beoordeeld. Daarnaast vindt periodiek, minimaal één keer per jaar, voor het laatst in maart 2023, overleg plaats met de externe IT-beheerder om ervoor te zorgen dat het beleid inzake gegevensbescherming, de standaarden en procedures actueel en marktconform zijn. Indien nodig zullen wijzigingen in het beleid worden aangebracht.

14 Toegang tot IT-systemen en toegang op afstand

14.1 Heeft Bell een procedure om ongepaste of niet-geautoriseerde IT-activiteit te ontdekken en te managen?

De externe IT-beheerder van Bell monitort continue de activiteiten in de Microsoft cloud en op laptops. Ernstige alarmeringen en verdacht verdrag worden door de externe IT-beheerder direct gerapporteerd aan de SPO.

14.2 Hoe garandeert Bell dat haar werknemers de juiste toegangsrechten tot de IT-systemen hebben?

Bell heeft voor nieuwe werknemers een instructie voor de toegang tot het netwerk. De klant-verantwoordelijke adviseur bepaalt wie toegang tot de gegevens van de klant heeft. In uitzonderlijke situaties kunnen gebruikersrechten worden gewijzigd

na autorisatie door de SPO. Ons systeem voor gegevensopslag is een gesloten system, waarbij toegang tot een klantbestand beperkt is tot werknemers van Bell die over de juiste autorisatie beschikken en de toegang nodig hebben ter uitvoering van de dienstverlening aan de klant.

14.3 Welke oplossingen gebruikt Bell om haar werknemers toegang op afstand tot haar netwerk te bieden?

Externe toegang op afstand is mogelijk via zakelijke laptops die door de externe IT-beheerder daarvoor zijn geautoriseerd, na goedkeuring door de SPO. Toegang is beveiligd middels gebruikersnaam en wachtwoord.

Naast deze zakelijke laptops is toegang alleen mogelijk via privé laptops en smartphones op basis van “Conditional Access” waarbij sprake is van een tweestapsverificatie.

15 Beveiliging

15.1 Welke beveiliging wordt toegepast om laptops en netwerk van Bell te beveiligen?

Gegevensopslag vindt plaats binnen de Microsoft cloud. Alleen geautoriseerde werknemers van Bell hebben toegang tot de opgeslagen gegevens. Alle op Microsoft 365 gebaseerde systemen zijn voorzien van antivirussoftware, welke automatisch wordt bijgewerkt zodra nieuwe bescherming beschikbaar komt. Alle Microsoft 365 systemen worden bijgewerkt zodra nieuwe veiligheid patches van Microsoft of andere softwareleveranciers beschikbaar komen. Anti-virus en anti-spam software scant alle externe e-mail. Specifieke software wordt gebruikt om specifieke binnenkomende e-mail te kunnen blokkeren en domeinen van afzenders te kunnen controleren. Internet websites worden gescand op kwaadwillige inhoud. Laptops zijn beschermd tegen ongeautoriseerd gebruik en verdacht bestandsgedrag. Alle data die op laptops staan zijn encrypted.

15.2 Voert Bell toegangscontroles op haar netwerk en systemen uit, en zo ja, hoe vaak?

De externe IT-beheerder voert continu standaard controles uit op het netwerk en de systemen van Bell. Ernstige alarmeringen worden door de externe IT-beheerder direct gerapporteerd aan de SPO en het management van Bell.

15.3 Gebruikt Bell draadloze netwerken? Hoe zijn deze beveiligd?

Bell beschikt alleen over een bedraad bedrijfsnetwerk, en niet over een gastennetwerk. Toegang tot het bedrijfsnetwerk is beperkt tot Bell-laptops, waarbij toegang alleen is toegestaan voor geautoriseerde laptops. Zie verder 14.3.

15.4 Welke technische en organisatorische maatregelen zijn door Bell getroffen om klantgegevens binnen haar kantoor te beveiligen?

Alleen werknemers hebben een sleutel waarmee zij toegang tot het kantoor krijgen. Bezoekers worden toegelaten tot de vergaderruimte, maar hebben geen niet-begeleide toegang tot andere ruimtes waar klantgegevens aanwezig zouden kunnen zijn. Vertrouwelijke documentatie op papier wordt periodiek gearchiveerd. Documenten die niet worden gearchiveerd of opgeborgen worden vernietigd. Vertrouwelijke documenten worden opgeborgen in afgesloten kasten. Laptops bevatten alleen versleutelde gegevens.

15.5 Hoe worden partijen die toegang hebben tot systemen met klantgegevens of deze managen, gecontroleerd?

Bell heeft een contract met haar externe IT-beheerder waarin het handhaven van de informatiebeveiliging is geregeld. Incidentele veiligheidseisen worden separaat geregeld via aanvullende veiligheidsprocedures afgestemd op die

specifieke omstandigheden. Andere partijen hebben geen toegang tot onze klantgegevens.

16 Versleuteling

16.1 Hoe worden klantgegevens naar externe partijen verzonden en wordt daarbij gebruikt gemaakt van versleuteling?

Via email worden persoonsgegevens verzonden met behulp van met een wachtwoord beveiligde zip-bestanden. Het wachtwoord wordt indien mogelijk via een ander medium dan email (zoals telefonisch, via sms of WhatsApp) aan de rechtmatige ontvanger van de file verzonden. Bell onderzoekt mogelijkheden om het uploaden en downloaden van klantgegevens mogelijk te maken via een beveiligde webpagina. De externe verzender/ontvanger ontvangt een link naar die pagina, en krijgt met behulp van het juiste wachtwoord, eenmalig de mogelijkheid voor een upload of download.

16.2 Hoe worden mobiele gegevens versleuteld?

Alle Bell laptops zijn volledig versleuteld.