pension consultants
& actuaries

How we protect clients' data

May 2022

Data protection Bell Pension Consultants & Actuaries B.V.

This note sets out the controls Bell Pension Consultants & Actuaries B.V. (hereafter: Bell) has in place to protect clients' data and to comply with data protection legislation. It also sets out the steps that Bell has taken to ensure compliance with the General Data Protection Regulation (GDPR), as laid down in the Dutch "Algemene Verordening Gegevensbescherming" (AVG), in force from 25 May 2018. The note has been produced in response to questions asked by clients. We will update it from time to time, to reflect changes in our procedures and policies, the last update being in May 2022.

pension consultants
& actuaries

Content

13.2 Are Bell's data security policies and procedures reviewed by internal or external auditors?

14 Access to IT systems and remote access

14.1 Does Bell have a process for detecting and managing inappropriate or unauthorised IT activity?

14.2 How do you ensure that Bell's partners and staff (including contractors) have the correct level of access to IT systems?

14.3 What solutions does Bell use for partners and staff to gain remote access to the network?

15 Security

15.1 What information security technology controls are in place to protect Bell's computers and networks?

15.2 Does Bell perform security penetrating testing on your network and systems? If so, how frequently?

15.3 Does Bell use wireless networks? How are they secured?

15.4 What technical and organisational security measures are in place to protect the security of clients' data within Bell's offices?

15.5 What measures are in place at the data centres where client data is stored?

15.6 How often do you assess third parties who have access to or manage systems supporting clients' information?

16 Encryption

16.1 How is data transmitted outside Bell and is encryption used?

16.2 How is mobile data encrypted?

1 AVG

1.1 How is AVG embedded within Bell?

Bell has a Data Protection Officer (DPO) who is responsible for taking AVG compliance forward. The DPO is regularly assessing our processes against the AVG, identifying each process that handles personal data and identifying any areas for development. This involves updating policies, privacy notices, procedures and client agreements and provide any additional training to ensure AVG compliance for now and the future.

1.2 What training is Bell providing to partners and staff on compliance with the AVG?

Data protection is a permanent agenda item during the regular team meetings of Bell. Bell requires all partners and staff to be trained in data protection. All employees of Bell are obliged to sign a AVG-protocol to declare they are familiar with the procedures concerning data protection and to act in compliance with the AVG.

2 Governance

2.1 What is Bell's data governance framework and who within Bell is responsible for data protection?

Bell has a data governance framework in place to ensure it can store and process its client data securely and appropriately. Bell's DPO is responsible for the data protection policy. Within the regular team meetings, the policy and implementation will be discussed on a regular basis. If necessary improvements will be implemented.

3 Security policies

3.1 Does Bell have a Data Protection Policy?

Bell has several data protection policies in place, for example covering: acceptable use of assets, data protection impact assessment, mobile devices, information classification, passwords, clear desk and data breach response.

4 Employees

4.1 Does Bell perform pre-employment screening for all new personnel including criminal and credit checks?

Bell carries out background checks for all candidates for employment (both permanent and contract). This includes: address verification, employment history, academic history, professional qualifications and a Statement of Conduct. We also contact previous employers.

4.2 Are all personnel required to sign an NDA or confidentiality agreement as a condition of employment to protect client information?

Yes.

5 . Training

5.1 Do Bell's partners and staff undertake security awareness and data protection training?

All partners and staff undertake security awareness training and data protection awareness training when they join Bell. All partners and staff are required to undertake data protection compliance training at least every three years. Bell has documented security policies which are available to all partners and staff. Partners and staff are reminded and updated about these policies via regular team meetings.

6 Location of Bell's data

6.1 Is Bell's data held outside of The Netherlands? What controls are in place to ensure client data is not transferred out of the EEA?

Client data is stored in the Private Cloud of our IT Administrator. This Private Cloud is vested in a data centre in The Netherlands. In two other data centres, also in The Netherlands, real time copies are stored. Bell does not store any client or member data in any country outside The Netherlands. These data is only accessible with correct authorisation.

7 Data processing

7.1 How do you ensure that data processed by Bell on behalf of your clients is limited to what is necessary for the agreed purpose?

When we are appointed, or for each material piece of work, we agree with our client the purpose and objective of the work and the data items required.

7.2 Does Bell process client data for any different purposes to that for which it was originally collected?

There may be some special cases where we process data for purposes different to which it was originally collected in order to enhance the service we provide to clients. In cases such as these, where possible, we will use anonymised or non-personal data. Where this is not possible and we are intending to use the data for a purpose not initially envisaged, we will obtain clients' explicit agreement to this. There may also be some special cases where we are required to process data in order to meet a particular statutory requirement, for example where we are required to disclose information to a regulatory body. We will immediately inform our client about such request.

7.3 What special provisions does Bell have in place to protect "sensitive personal data"?

Bell does not process sensitive personal data as intended in article 9 of the AVG , nor criminal nature data as intended in article 10 of the AVG. Therefore, special provisions are not necessary.

7.4 Does Bell use processing agreements and which arrangements will be made in this case with the responsible party of the processing?

In case we give advice regarding a client's collective pension plan or regarding the selection of specific pension products (including disability insurances), a data processing agreement (DPA) is not applicable. Bell does not act as a processor but as a controller. Processing client's data is no primary business for Bell, it is merely a logical result of the services of Bell to her clients. It's our independent decision which data is required and how we process this data. Of course, as controller we are also obliged to be careful when processing data of clients. In this note we describe how Bell complies with data protection legislation.

In case of specific circumstances, a DPA can be applicable. In that case, in consultation with the client a DPA will be will drafted and signed, as part of the agreement between the client and Bell.

7.5 Does Bell use sub processing agreements and which arrangements will be made in this case with the sub processor?

Generally Bell does not make use of a sub processor. In case we would like to make use of a sub processor, we will ask for the approval of the client beforehand. In that case, we do require a statement from the sub processor declaring that he will act in compliance with the AVG.

8 Breaches and security incidents

8.1 Has Bell had to report any data security breaches to the Dutch Data Protection Authority (DPA)? Has Bell been the subject of any investigation or enforcement action from the DPA?

No data security breaches have been reported to the DPA by Bell. Bell has not been the subject of any investigation or enforcement action from the DPA.

8.2 How are data protection breaches and incidents managed within Bell?

Bell has a data protection breach procedure that requires all data protection incidents to be reported to Bell's DPO who co-ordinates escalation, investigation and remediation accordingly. Bell has various alerting mechanisms in place to detect cyber incidents. Teams are notified of critical events (eg malware attack) via email. Bell also has a managed Intrusion Detection System to protect web based applications. Members of Bell's IT Administrator

receive notifications of threats that have been acted upon and these are passed on to the DPO. All devices of Bell have End Point Protection. The software ensures malware is detected and deleted automatically. Via this software it's also possible to recover files after a ransomware attack. A forensic report will be drawn to show what happened and where the breach took place.

8.3 What processes are in place to ensure clients are informed of data protection breaches?

Where a data protection incident may have an impact on a client's data, the client partner would notify the client contact concerned and carry out a timely investigation with the DPO. This investigation is part of Bell's Data Protection Breach Procedure (see paragraph 8.2).

9 Subject access requests

9.1 How does Bell manage subject access requests?

Bell has a written policy for dealing with subject access requests. We have ensured it reflects the requirements under the AVG. Subject access requests are sent to the DPO to log and take forward.

10 Business continuity

10.1 What provisions does Bell have in place to deal with a significant cyber security event?

The most important provision made by Bell is storing all clients' data in an external secured data centre. Therefore, Bell can log on via secure Virtual Private Network (VPN) to her system from any place outside the office and continue her services with as little as possible nuisance for the clients. In case a data centre fails, an almost immediate switch to one of the other two data centres is realised.

11 Backups and data retention

11.1 How is clients' data backed up? Does Bell have the capability to recover data for a specific client in the event of failure or data loss?

Bell's systems are backed up daily. Backups are stored offside in the external data centre. Backups that are recalled from offsite storage can only be accessed on the authority of specified Bell personnel. In case of a system failure or data loss in the data centre the data will be recalled from one of the other data centres.

11.2 What is Bell's policy on data retention?

Bell retains data for so long as is necessary to meet our legal, regulatory and professional obligations.

11.3 What is Bell's procedure for dealing with requests to correct/delete clients' data?

We will action clients' requests to correct the data we hold for them where possible. We will action clients' requests to delete data provided this is in line with our policies or where other special terms have been mutually agreed.

12 Disposal

12.1 What controls are in place to securely dispose of clients' information on paper?

Client data on paper is placed in Bell's secure bins and collected by a vetted company.

12.2 What controls are in place to securely dispose of portable media and the decommissioning of servers and devices that contain clients' information?

Bell engages specialist companies who certify the destruction of all data from all computer hardware that is disposed of (including disks, servers, workstations, backup tapes). Mobile phones are wiped of any data before being transferred to another user or being retired.

13 Audit and accreditation

13.1 What information security standards does Bell hold?

Bell doesn't have any certificates concerning data security. The data centres in which our clients´ data is stored are ISO27001 certified.

13.2 Are Bell's data security policies and procedures reviewed by internal or external auditors?

Our data security policy is audited internally. Besides this, we have a periodical meeting at least once a year with our external IT Administrator to ensure our policy about data protection, standard and procedures are up to date and in conformity with market practices. In preparation to this meeting our IT Administrator performs a Security scan. If necessary our data protection policy will be renewed.

14 Access to IT systems and remote access

14.1 Does Bell have a process for detecting and managing inappropriate or unauthorised IT activity?

Our IT Administrator monitors userfile activity on the fileserver, laptops and mobiles, and reports on a monthly basis. Critical alerts are directed immediately to the DPO. Our mobile devices are managed by Mobile Device Management.

14.2 How do you ensure that Bell's partners and staff (including contractors) have the correct level of access to IT systems?

Bell has a documented new joiner procedure that sets out base network access requirements. Team leaders control access to their clients' data based on team requirements. In special circumstances user access rights can also be modified after authorisation by the DPO. Our standard electronic client filling system is a "closed" system. Accordingly, access to each client file is restricted to Bell personnel who need to have access to that information for the purposes of servicing the client. System passwords are restricted to relevant and authorised personnel only.

14.3 What solutions does Bell use for partners and staff to gain remote access to the network?

External remote access is only possible via Virtual Private Network (VPN). Usage is restricted after approval by the DPO. Access is protected via usernames and passwords.

Bell has a Mobile Device Management solution that secures data and access to encrypted portions of the device. Enforced security policies prevent unauthorised access including through remote locking and erasing of the device.

15 Security

15.1 What information security technology controls are in place to protect Bell's computers and networks?

Bell's network perimeter is secured with firewalls and intrusion prevention systems. Only authorised Bell personnel can access Bell's systems. All Microsoft Windows based systems are protected with anti-virus software which is automatically updated with new protection as it becomes available. All Microsoft Windows systems are subject to security patching from Microsoft and other third party vendors. All external email is scanned by a system providing anti-virus and anti-spam protection. Additional email scanning policies prevent certain email content entering the network. Internet access is restricted to approved website categories and websites are scanned for malicious content. Desktops and laptops are further protected with technology to prevent unauthorised intrusion and block suspicious fie behaviour.

15.2 Does Bell perform security penetrating testing on your network and systems? If so, how frequently?

A certified ethical hacker, employed by our IT Administrator, regularly investigates our IT-system looking for security errors. Shortcomings will be

discussed between the IT Administrator and the DPO Critical alerts are directed immediately to the DPO.

15.3 Does Bell use wireless networks? How are they secured?

Bell has segregated corporate and guest wireless networks. Bell's corporate wireless network is restricted to Bell computers only - access is restricted to authorised computer, user and security certificates.

15.4 What technical and organisational security measures are in place to protect the security of clients' data within Bell's offices?

All partners and staff have their own key which enable them to access the office work areas. Visitors to the premises are escorted to meeting rooms and do not have unescorted access to other areas where client's data can be stored. All confidential paper documentation is archived on a regular basis. All documents that are not filed or stored are placed in confidential waste bins for shredding. Confidential documents are stored securely in locked cabinets. All data stored at desktop computers is encrypted.

15.5 What measures are in place at the data centres where client data is stored?

The three data centres managed by our IT Administrator are connected redundantly with each other. In case a data centre fails, a switch to one of the other data centres will be made immediately. The data centres in which our clients´ data is stored are ISO27001 certified.

15.6 How do you assess third parties who have access to or manage systems supporting clients' information?

A contract to maintain information security is in place with the IT Administrator. Additional security requirements are agreed on a case-by-case basis to ensure adequate information security procedures are in place for the specific circumstances. Other third parties have no access to our clients' data.

16 Encryption

16.1 How is data transmitted outside Bell and is encryption used?

All partners and staff are trained to password protect sensitive information prior to emailing. Client's data is transmitted via zipped password protected files. The password is - if possible - send separately to the receiver via an independent medium (like by phone, sms or WhatsApp). In short term Bell will facilitate to upload and download of data via a protected webpage. The external sender/receiver will receive a hyperlink to this webpage, and only with a valid password they are enabled once to upload or download the necessary data.

16.2 How is mobile data encrypted?

All Bell laptops are encrypted (full disk encryption) and are automatically locked out after multiple incorrect passwords.