PRIVACY STATEMENT FOR ABN AMRO EMPLOYEES

This Privacy Statement was amended on 24 February 2023.

1. General

This Privacy Statement applies to all employees of ABN AMRO. For the purpose of this Privacy Statement, 'employees' means employees who are employed by ABN AMRO Bank N.V. and work for ABN AMRO or one of its subsidiaries. This Privacy Statement also applies to external employees who are hired by the Bank as agency staff or are on secondment. For the sake of convenience, the terms 'the Bank' and 'employees' are used in the rest of this Privacy Statement.

We also to refer to the Personal Data Policy, which sets out the internal rules on the processing of personal data relating to clients, employees and other individuals whose personal data is processed by the Bank.

1.1 Who is responsible for your personal data?

As your employer, the Bank is responsible for your personal data. The Bank means:

ABN AMRO Bank N.V

Gustav Mahlerlaan 10

1082 PP Amsterdam, The Netherlands

Amsterdam Chamber of Commerce, Trade Register number 34334259

1.2 Data Protection Officer

The Bank has a Data Protection Officer. The Data Protection Officer monitors the application of, and compliance with, the GDPR at ABN AMRO. The role of Data Protection Officer comes under the Privacy Office.

1.3 What is personal data?

This Privacy Statement explains how the Bank uses your personal data. But what exactly is personal data? The best-known forms of personal data are your name, address, age and date of birth. Personal data also includes work email addresses, telephone numbers, bank account numbers and your national identification number. There are several special categories of personal data. They consist of personal data that is so sensitive its use may seriously affect an individual's privacy. These include data concerning your health, sexual orientation, cultural background or trade union membership. Biometric data is also considered to be a special category of personal data. It encompasses a variety of ways in which an individual's physical features are measured and identified. Examples include fingerprints (e.g. for gaining access to secure areas). Data protection legislation imposes strict requirements on the use of special categories of personal data.

2. Basis and purposes

2.1 On what basis does the Bank process your personal data?

The Bank must have a reason for asking for or using your personal data. This is referred to in the law as 'a legal basis for processing' your personal data. As your employer, the Bank uses your personal data if it has one or more of the following legal bases for doing so.

- **Agreement**
  The Bank uses your personal data where necessary to comply with the employment agreement concluded with you.

- **Legal obligation**
  In addition, the Bank processes your personal data because it is required to do so under various laws and regulations.

- **Legitimate interest**
  The Bank or another party also has the right to use your personal data if this is in its own interest. This is referred to as a 'legitimate interest'. For this to apply, the Bank or other party's interest in using your personal data must outweigh your right to privacy. In situations such as these, the Bank balances all the interests. Examples of the Bank's legitimate interest in using your data include protecting the Bank's integrity and security and pursuing a responsible, effective and efficient HR policy.

- **Vital interest**
  There may be cases in which the Bank uses your personal data because this is necessary to protect your life or that of another person, for instance if the Bank has to share personal data relating to you with a hospital.

2.2 Using personal data with your consent

The Bank will not ask you to consent to the use of your personal data apart from in exceptional situations. If you have given consent you can withdraw it at any time. Withdrawing your consent may have consequences, however. If, for example, you have consented in an app to the use of information concerning your location, withdrawing your consent may mean that the app works differently.

2.3 Does the Bank also use personal data relating to you that it did not obtain from you directly?

Yes, the Bank also uses personal data relating to you that it did not obtain from you directly. Personal data may be obtained from sources such as:

- An employment or recruitment agency (for instance your name and address for the purpose of concluding a secondment agreement)
- Public registers that contain your personal data, such as the Trade Register of the Chamber of Commerce and the Dutch Land Registry

- UWV
- The occupational health and safety service
- An external agency that is engaged in the context of reintegration or career guidance
- In the context of in-employment screening (see point 2.4 of the section headed '**What does the Bank use your personal data for?**'), we may request references from former employers specified by you, and the Bank may make use of public sources such as search engines and public sections of social media accounts.
- The Financial Institutions Incident Warning System Protocol (*Protocol Incidentenwaarschuwingssysteem Financiële Instellingen*). Section 2.4.3 contains a brief explanation of how this warning system works. For more information about this warning system and its workings, please visit the website of the Dutch Banking Association (NVB): website of Dutch Banking Association.

2.4 What does the Bank use your personal data for?

As your employer, the Bank uses your personal data for the following purposes.

2.4.1 Obligations under legislation and regulations.

The Bank uses personal data relating to employees in order to comply with applicable legislation and regulations, Examples include:

- MiFID II. The Bank is required to record conversations between advisers and clients that concern investing. For more information, please refer to the Voice Logging & Video Regulations.
- Tax laws. By law, the Bank must share specific information relating to its employees with the Dutch Tax and Customs Administration. For example, the payroll tax form submitted to the Dutch Tax and Customs Administration includes each employee's citizen service number (BSN), date of birth, address and nationality.
- Dutch Code of Civil Procedure. If someone garnishes your wages, the Bank, as your employer, is under a legal obligation to cooperate in this and provide information about you to the bailiff.
- Financial supervision regulations. In some situations the Bank has to provide personal data relating to employees to a supervisory authority in the context of an examination under supervisory law or in the context of a licence application.
- Dutch Criminal Code. The Bank may be required to provide personal data relating to employees to investigation services in the context of a criminal investigation.
- Foundation for Banking Ethics Enforcement. If you are involved in an incident, the Bank may be required to report this to the Foundation for Banking Ethics Enforcement (Stichting Tuchtrecht Banken).
- Sometimes the Bank has to supply personal data as part of court proceedings or following a request from competent authorities (at a national or international level).
- Social security law. Sometimes the bank is required to share information with UWV, for example if you have been on sick leave for a long time or if you are pregnant.

2.4.2 Employment agreement

The Bank needs your personal data for the conclusion and performance of its employment agreement with you. In this context, examples of the purposes for which the Bank processes your personal data include:

- paying your salary;
- processing the Employee Benefits you use;
- recording absences;
- training and appraising employees, including as part of the Bank's Together & Better programme;
- for the pension scheme.

2.4.3 Ensuring integrity and security

The Bank uses personal data to protect itself, its property, its data and its employees from all kinds of breaches, damage and losses insofar as possible. Examples include:

- Security cameras within the Bank's buildings and in their surroundings. For more information about the use of camera surveillance within the Bank, please see the CCTV Monitoring Rules.
- Additional security measures are in place in some of the Bank's buildings and spaces, such as the Computer Centres in Amstelveen: a scan of your fingerprint will be processed if you are given access to certain rooms in that building. Since this form of security is essential for the Bank, biometric data of this kind may be used on the basis that the Bank has a legitimate interest.
- If you want to access the ABN AMRO network using your mobile device, your device will be scanned by a security tool (Defender MTD). This is done to protect our data and client data against cybercrime attacks from mobile devices. More information about Defender MTD and the use of personal data can be found on the intranet.
- If you have been involved in an incident, or if it is suspected that you have been involved in an incident, the Bank will perform an investigation and may use your personal data in this context. Examples of incidents include undesirable behaviour (such as harassment or discrimination, sexual or otherwise) or unauthorised use of the Bank's systems. SIM is the central point of contact for crime and security incidents that may affect the integrity and performance of the Bank, our clients and our employees. The Bank has rules of conduct with which employees must comply. To view them, go to General rules of conduct (sharepoint.com).
- The Bank performs in-employment screening. This means that you undergo screening when you start as an employee and also if you switch to a role for which a different or more stringent form of screening is required. Personal data obtained from public sources may also be used for this purpose.
- In the context of security, the Bank may monitor activity on your computer, including your emails from your ABN AMRO work email address.
- If your role involves chat sessions with Bloomberg and Reuters, or if your role is covered by the MiFID II rules, the Bank may monitor your chat sessions. See also the explanation provided in section 2.5.1 Monitoring. In this context, you are advised to read the Rules on Monitoring Emails and Chat Sessions.
- To help ensure the security and integrity of the Bank and our sector, the Bank may use your personal data in the internal and external reference registers. A more detailed explanation of these warning systems is provided below.

Warning system used by the Bank

Imagine that a client or employee is involved in damage to, or the loss of, our property, or that there are suspicions that a client or employee has committed fraud, or that a client or employee is being investigated by the authorities or the police.

These are all examples of incidents to which the Bank must pay special attention. The Bank must be able to record and remember these incidents so that it can take appropriate measures or further action. The Bank has a legitimate interest in this.

Incidents of this kind are referred to as “events". These events are recorded in a special internal record kept by the Bank, generally referred to as "event records", which can only be accessed by authorised employees. Events records are kept on clients as well as employees. An explanation of how we do this for employees is provided below.

The internal reference register

An internal reference register (Dutch acronym: IVR) is linked to the event records. The internal reference register allows us to warn the appropriate departments and group companies within ABN AMRO in situations where we believe an employee's involvement in an event is sufficiently serious. This warning does not have any effect outside our organisation. We check the GDPR rules to determine whether it is permissible to share a specific event through the internal reference register within our organisation. When a client is included in this register, we provide specific information about the reasons for the inclusion in the internal reference register, the consequences of inclusion for the employee and also the employee's relationship with us and our group companies, as well as the duration of the inclusion and the employee's rights, such as the right to object.

The external reference register (ERR)

In addition to this, financial institutions in the Netherlands, including ABN AMRO, have developed a warning system that, in contrast to the event records and internal reference register, also has an effect externally.

This system allows the financial institutions to check whether a person:

- has ever committed fraud,
- has tried to commit fraud,
- or somehow forms a threat to the safety and security of the banking sector. This system is also applicable to clients. Other banks affiliated with the Dutch Banking Association also use this system, which is why you can read more about this warning system and how it works on the website of the Dutch Banking Association and the website of the Dutch Data Protection Authority. The rules governing how banks, and therefore ABN AMRO, can use the external warning system have been approved by the Dutch Data Protection Authority. These rules can also be found on the website of the Dutch Banking Association. If you are included in this external warning system, you will be provided with information about your inclusion in the register and how to exercise your data protection and other rights.

When you apply to work for us, we check the internal and external reference registers. Only persons who handle client acceptance, product acceptance and employee acceptance are permitted to check these lists. These employees will only be alerted by a signal if you are included in the register. Only a

limited number of authorised employees have access to details of the reasons for inclusion in the lists. This information is always used as a basis for assessing whether the Bank can accept an employee and determining the applicable conditions.

2.4.4 Efficient, optimum use of facilities, such as IT, workstations and buildings

The Bank uses personal data to provide employees with the necessary facilities in the most effective way possible, Examples include:

- Spreading employees across spaces and buildings, for example when employees reserve meeting rooms or parking spaces or are looking for a free workstation. For instance, Wi-Fi signals may be used to monitor which workspaces are occupied. In addition, the bank uses your access pass to keep track of your presence in the building and analyse workplace occupancy. Analyses are performed to check that the actual use of the building is in line with its intended use.
- Monitoring the use of IT equipment, such as video conferencing equipment and printers, or the use of software packages on laptops belonging to ABN AMRO.

Alongside monitoring, data relating to the users of the facilities user may also be used in statistical and other studies looking at the impact of specific facilities (including their use) and related policies on employees and business objectives. Examples include studies that examine which facilities contribute to improved services at ABN AMRO or how specific facilities contribute to the employee experience. The results of such studies can never be traced back to individuals.

2.4.5 HR management

The Bank uses personal data so that it can pursue a responsible, effective and efficient HR policy. This includes the following, among other things:

- Staff planning and the policy on the influx and outflux of employees.
- Policy on sick leave and reintegration.
- Subsidy application for employees who are at a disadvantage on the labour market.
- The products offered by HR, such as education and training.
- Measuring employee experience and employee engagement.
- Data analysis based on advanced statistical methods
    - Policy analyses: studies carried out to show the impact of HR strategy and policy on employees' objectives and business objectives. Examples of areas of research include the forms of training that have an impact on client satisfaction, and the key drivers of employee engagement within the organisation. A limited number of employees have access to this data owing to their roles. The results of such studies and the related recommendations can never be traced back to individual employees.
    - Personal analyses: In the context of HR services, personal data may be used to provide employees with personal advice, such as recommendations (optional or otherwise) for vacancies or training courses. See also the '[Personalised HR Services Module]' for more information about the conditions that apply.

- The Bank's diversity policy. The Bank seeks to ensure that greater diversity within society is reflected throughout the Bank. It therefore wants to monitor diversity in all levels of the organisation, so that it can develop intervention procedures if necessary. The Bank uses data about the gender, age and country of origin of employees for this purpose. A limited number of employees have access to this data owing to their roles. Moreover, the Bank uses this data at an aggregated level. By 'aggregated', we mean that the relevant personal data is not processed at the level of the individual. With respect to the country of origin, the Bank only uses personal data relating to employees who have volunteered this information for this purpose: you can enter your country of birth, or that of your father or mother, in MyHR. You can change or delete this personal data at any time.
- The Bank's inclusion policy: for example, the Bank uses health data made available by employees on a voluntary basis in order to apply for and maintain a certification mark that provides added value for the Bank and employees. Each employee is free to decide whether they will make their health data available for this purpose.

2.4.6 Improving and revamping services

- If you use a telephone belonging to the Bank for contact with clients for business purposes, the Bank may record your telephone calls, chat messages or (video) chat sessions with clients (we refer to this as logging) with the aim of improving the quality of those conversations. Examples include the work performed in the Contact Centre. See also the explanation provided in section 2.5.1 Logging.
- Reports and/or dashboards may be used to improve internal processes. The dashboards must not be used for the purpose of appraising employees unless a set of rules that has been approved by the Employee Council specifically indicates otherwise. For more information, see the Memo on personal data in reports and (online) dashboards at ABN AMRO.
- Innovation. Employees who are actively involved in the development of new technologies (DevOps, CISO) may test those tools while they are in development. Participation is conditional upon the safeguarding of the data protection rights of the employees in question. This is assessed on a case-by-case basis.
- Advanced technologies, such as artificial intelligence, are used to help employees carry out their work.

2.5 Logging and monitoring

As you will have gathered from the information provided above, the Bank uses various logging and monitoring techniques. What do logging and monitoring entail?

2.5 Logging

When the Bank logs information, it records the personal data so that it can view it at a later date, for example if the supervisory authority carries out an investigation. Certain logs may subsequently be used for monitoring purposes (for a more detailed explanation of monitoring, see section 2.5.2 Monitoring). The following are examples of logging:

- Recording who has had access to a specific space and when they had access (use of access pass, for example).

- Recording the telephone calls of employees working in the Contact Centre and the Dealing Room, in order to improve the quality of these calls.
- Capturing and recording of videos for the internal provision of information. For more information see Chapter 2 of the Voice Logging & Video Regulations.
- Recording who has had access (and when they had access) to applications containing confidential employee, client and/or product information and who changed or viewed what in those applications (see for more information: Audit Trial on employee and client data (Policy Number: S07-400)).
- Under European rules, the Bank is also required to record telephone calls between advisers and clients that concern investing.

For more information about logging, see the Voice Logging & Video Regulations.

We recommend that you read the following documents for more information on this topic:

- The rules of conduct governing the use of email, intranet and internet for business purposes: Use of email, intranet and internet (sharepoint.com).
- The Information Security Awareness and Secure Behaviour Policy.
- The Standard for Audit Trail on employee and client data

2.5.2 Monitoring

Monitoring is not the same as logging. When the Bank performs monitoring activities, it actively keeps a record of what happens in a specific place or within a specific channel (such as email) and intervenes if something goes wrong. For more information, see the Rules for Employee Tracking Systems.

The Bank monitors its employees for various purposes. We do not make any use of automated decision making in that context.

- **Security**: examples include monitoring emails and chat messages, monitoring the use of faxes, scanners and printers, and monitoring the saving of documents on a USB flash drive (in other words, the Bank monitors the saving of internal documents on external devices).
- **Compliance with legal obligations**: for instance, the bank's monitoring of securities transactions by employees depends on the relevant employee's compliance status.
- Efficient, optimum use of facilities, such as IT, workstations and buildings: Wi-Fi tracking, sensors, data relating to access passes and data relating to reservations. We do not look at this at the level of the individual.
- Measures to prevent employees gaining **unauthorised access to accounts**.

2.6 Does the Bank use your personal data for purposes other than the purpose for which it was initially obtained

The Bank may also use your personal data for a purpose other than the purpose for which you initially provided it. This is, however, subject to the condition that the new purpose must be in line with the purpose for which you initially provided your personal data to the Bank. To determine whether this is the case, the Bank looks at the following aspects as a minimum:

- Is this purpose clearly related to the purpose for which you initially provided the personal data? Is the new purpose appropriate to the initial purpose?
- How was the personal data originally obtained from you? Was the personal data obtained directly from you or in another way?
- What kind of personal data is concerned exactly? Does it concern sensitive information? or data that is not so sensitive?
- What would be the implications for you if the Bank were to use the personal data in another way? Would you benefit, suffer or neither?
- What can the Bank do to ensure the highest possible level of data protection when reusing your personal data? Examples include anonymisation and encryption.

2.7 Profiling

The Bank makes use of profiling. This is understood to mean putting people into groups (profiles). Profiling allows the Bank to evaluate and analyse personal aspects and make predictions. The situations in which the Bank uses employee's personal data for profiling and the reasons for this are explained below.

- **Preventing unauthorised transactions**
  The Bank monitors securities transactions by employees depending on their compliance status. The purpose of this monitoring is to prevent unauthorised transactions, such as insider trading. The Bank uses profiles for this purpose. A profile consists of characteristics which the Bank uses to identify unauthorised transactions. If potentially unauthorised transactions are detected, the Bank will carry out an investigation. If it is established that you have executed an unauthorised transaction, you may be dismissed with immediate effect.
- **Personalised HR services**
  The Bank may carry out analyses to personalise its services (see section 2.4.5 and the 'Personalised HR Services Module').

You have the right to object to the use of your personal data for profiling purposes. You can submit your objection through Contact HR (accessible through the intranet page for employees).

The Bank is not obliged to grant your request in all cases.

3. Sharing your personal data with third parties and transferring your personal data outside the EU

3.1 Does the Bank share your personal data with others?

Yes, in some situations the Bank has to share your personal data with others.

- **Pension fund and insurers**
  For example, the Bank shares personal data with ABN AMRO Pensioenfonds in order to make arrangements for your pension, and also with insurers, for instance when taking out insurance for a supplement to occupational disability benefit (WIA).

- **Occupational health and safety service**
  If you report sick, the fact that you are sick will also be reported to Beter, the Bank's occupational health and safety service (and subsidiary). The reason you are sick / on sick leave will not be mentioned.
- **National and international public authorities**
  There are some situations in which the Bank is required to disclose your personal data to public authorities such as the Dutch Tax and Customs Administration and UWV, and possibly also competent international public authorities. The Bank's supervisory authorities may also ask for data. The Bank must share data with them if it is required to do so by law, even if this data includes your personal data. The police may ask for camera images in which you appear in connection with an incident. The Bank will provide these images to the police if it is required to do so.
- **Foundation for Banking Ethics Enforcement**
  Persons employed in the financial sector are bound by the disciplinary law for banks in the Netherlands. In the context of disciplinary proceedings, personal data may be provided to the Foundation for Banking Ethics Enforcement (Stichting Tuchtrecht Banken).
- **Other companies**
  The Bank works with other companies. These companies may also require your personal data in order to perform their work for the Bank effectively. For example, your personal data might be required by KPN for the settlement of employee phone plans, or by Everbridge for the ABN AMRO Alert app, or by Pronk Geschenken for the Thumbs Up programme. The Bank takes due care when selecting the companies with which it works. The Bank reaches clear contractual agreements with these companies on how they are to handle your personal data. The Bank continues to be responsible for your personal data when it engages another company to carry out work on its behalf.

3.2 Is your personal data processed outside Europe too?

The Bank and its group companies may decide to share personal data with each other, even when the group companies are located outside Europe. For example, if you were to work for the Sydney office as an expat, the Bank would share personal data relating to you with that office so that you can be included in its systems. In doing so, the Bank must comply with the local rules.

The sharing of personal data with group companies outside Europe is governed by the Bank's global internal policy, the Binding Corporate Rules (BCRs). This policy has been approved by the Dutch Data Protection Authority.

The Bank may also make use of IT suppliers that are based outside Europe or that also offer services from countries outside Europe. In that case, the Bank will ensure that personal data is transferred in accordance with the data protection legislation.

4. Security and storage periods

4.1 Security of your personal data

The Bank does its utmost to ensure the highest possible level of protection for its employees' personal data. In connection with this, the Bank invests heavily in its people, systems and procedures. The way of

working is constantly geared to the sensitivity of the relevant data. Employees are trained how to keep data safe and secure.

For security reasons, details of the precise data protection measures taken by the Bank cannot be provided. Examples of the measures taken by the Bank to protect the personal data of employees can be found under point 2.4.3 of the section headed 'What does the Bank use your personal data for?' Other security measures you may have come across include:

- access to the Bank's systems using login codes or even two-step verification;
- restricted access to personal data: personal data can only be accessed by authorised individuals;
- requirements for sending confidential documents.

4.2 How does the Bank determine the period for which your personal data is stored?

The Bank stores personal data relating to you, such as your HR file (including your employment agreement and official appraisals), emails, chat session history and documents produced by you (including documents which do not relate to contact with clients).

When determining the storage periods for such personal data, the guiding principle followed by the Bank is that it must keep the personal data for at least as long as is necessary in order to fulfil the purpose for which that personal data was obtained. The following information is also relevant in this context.

- The data protection legislation does not stipulate specific storage periods for personal data. Other legislation may specify minimum retention periods, however. If it does, the Bank must observe these periods. Examples of such legislation include the Dutch Civil Code, tax laws and financial legislation such as MiFID II and the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme - Wwft).
- If the Bank becomes involved in a lawsuit or other legal proceedings in the Netherlands or in another country, the Bank may use data that includes personal data relating to you (such as emails from you relating to the dispute) in order to prove its case. The Bank may store this personal data in an archive until any claims have expired and legal proceedings can no longer be brought against it.

The Bank has formulated storage periods for several categories of personal data in the Local Retention Schedule (an appendix to the Bank's Data Retention Policy).

5. What rights do you have?

- **Right of access and right to rectification**
  You have the right to access the personal data relating to you that the Bank processes. You can also ask the Bank to correct any inaccuracies in your personal data. You can view and change much of your personal data yourself in MyHR, My Compliance, My Learning, Sharepoint and Talent2Grow. If you have an additional request, you can submit this through Contact HR (on the intranet page for employees).
- **Right to be forgotten**
  In some cases, you can also ask the Bank to delete your personal data. The Bank is not obliged to grant your request for the deletion of your personal data in all cases. For example, it is not under an obligation to do so if the law requires it to keep your personal data for a longer period of time.
- **Right to object**
  You may object to the use of personal data relating to you that is processed on the basis of the Bank's legitimate interest. The Bank is not obliged to stop processing your personal data in all cases. For example, it does not have to do so if it has an interest that outweighs the employee's interest.
- **Right to restriction of processing**
  You can also ask the Bank to restrict the use of your personal data on a temporary basis. This is possible in the following situations:
    - You think that your personal data are incorrect;
    - The Bank uses your personal data wrongfully;
    - The Bank wants to destroy your personal data (for instance after the storage period has ended) but you still need it.

You can also submit objections and requests for the deletion of your personal data or the restriction of its processing through Contact HR. Always clearly indicate the reason for your request.

More information about your rights and how to submit a request can be obtained from Contact HR. You can use the contact form on the Contact HR intranet page, or call +31 (0)20 343 60 00 on working days between 9 a.m. and 6 p.m.

- **Right to data portability**
  The Bank can arrange for you to obtain your personal data that you provided to it and which is stored by automated means. The Bank will not do this unless it processes your personal data on the basis of your consent or the employment agreement or contract it has concluded with you. This is referred to as data portability. You can also ask the Bank to transfer your personal data directly to another party, such as a subsequent employer.

Requests to receive your personal data or provide it to another party can be submitted through Contact HR.

Please keep your personal data secure. Check whether any party you want to provide your personal data to can be trusted and keeps your personal data as safe as the Bank does. If you want to receive your personal data, please make sure that your own equipment is adequately secure and has not been, and cannot be, hacked.

If you have questions, are unclear about anything, or want to make a complaint, please get in touch with HR through Contact HR. If you are not happy with the conclusion, you may contact the Data Protection Officer by sending an email to privacy.office@nl.abnamro.com. You also have the right to submit a complaint to the Dutch Data Protection Authority.

6. Changes to the Privacy Statement

The way your personal data is used may change over time due to changes in laws and regulations or in internal procedures or systems that will directly affect the Bank's use of your personal data. If this happens, the Privacy Statement will be changed and the Bank will notify you of these changes. In that case, the changes will be announced on the intranet. Former employees wishing to read the Privacy Statement can get in touch with Contact HR or call +31 (0)20 343 60 00 on working days between 9 a.m. and 5 p.m.