AP | bescherming in een digitale wereld

Date
02 March 2026

Our reference
2023-300387

Contact

070 8888 500

Subject
Decision approving Controller Binding Corporate Rules of ABN AMRO Bank

The Autoriteit Persoonsgegevens,

Pursuant to the request by **ABN AMRO Bank N.V.**, on behalf of the group **ABN AMRO Bank N.V.** (hereinafter '**ABN AMRO Bank**'), received on **21 June 2018**, reference **z2018/15470**, for approval of their binding corporate rules for controller;

Having regard to Articles 47, 57 and 64 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR);

Having regard to the judgment of the Court of Justice of the European Union in Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, C-311/18 of 16 July 2020;

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021;

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023 (hereinafter "the Recommendations 1/2022");

Makes the following observations:

1. Article 47(1) of the EU General Data Protection Regulation 2016/679 (GDPR), provides that the competent Supervisory Authority shall approve Binding Corporate Rules (BCRs) provided that they meet the requirements set out under this Article.

2. The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees to controllers and processors established in the EU as to the

protection of personal data that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country.

3. Before carrying out any transfer of personal data on the basis of the BCRs to one of the members of the group, it is the responsibility of any data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country of destination in the case of the specific data transfer, including onward transfer situations. This assessment has to be conducted in order to determine whether any legislation or practices of the third country applicable to the to-be-transferred data may impinge on the data importer's and/or the data exporter's ability to comply with their commitments taken in the BCR, taking into account the circumstances surrounding the transfer. In case of such possible impingement, the data exporter in a Member State, if needed with the help of the data importer, should assess whether it can provide supplementary measures in order to exclude such impingement and therefore to nevertheless ensure, for the envisaged transfer at hand, an essentially equivalent level of protection as provided in the EU. Deploying such supplementary measures is the responsibility of the data exporter and remains its responsibility even after approval of the BCRs by the competent Supervisory Authority and as such, they are not assessed by the competent Supervisory Authority as part of the approval process of the BCRs.

4. In any case, where the data exporter in a Member State is not able to implement supplementary measures necessary to ensure an essentially equivalent level of protection as provided in the EU, personal data cannot be lawfully transferred to a third country under these BCRs. In the same vein, where the data exporter is made aware of any changes in the relevant third country legislation that undermine the level of data protection required by EU law, the data exporter is required to suspend or end the transfer of personal data at stake to the concerned third countries.

5. In accordance with the cooperation procedure as set out in the Working Document WP263 revo1,[1] the Controller BCRs application of **ABN AMRO Bank** was reviewed by the Autoriteit Persoonsgegevens as the competent supervisory authority for the BCRs (BCR Lead) and by two Supervisory Authorities (SA) acting as co-reviewers, *in this case the Lithuanian and German (Hessen) SAs*. The application was also reviewed by the concerned SAs to which the BCRs were communicated as part of the cooperation procedure.

6. The review concluded that the Controller BCRs of **ABN AMRO Bank** comply with the requirements set out by Article 47(1) of the GDPR as well as the Recommendations 1/2022 and in particular that the aforementioned BCRs:

[1] Endorsed by the EDPB on 25 May 2018.

i) Are legally binding and contain a clear duty for each participating member of the Group including their employees to respect the BCRs by entering in an Intra-Group Agreement *(Section 5 of the application form and Article 3 of the BCRs);*

ii) Expressly confer enforceable third-party beneficiary rights to data subjects with regard to the processing of their personal data as part of the BCRs *(Articles 22 and 24 of the BCRs);*

iii) Fulfil the requirements laid down in Article 47(2) of the GDPR:

a) The structure and contact details of the group of undertakings and each of its members are described in the Application form of the Recommendations 1/2022 that was provided as part of the file review in *Section 5 of the application form;*

b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question are specified in *Annex B to the BCRs;*

c) the legally binding nature, both internally and externally, of the Controller BCRs is recognized in *Article 3 of the BCRs*;

d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules are detailed in *Articles 5, 11-13, 16 and 18 of the BCRs;*

e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22 of the GDPR, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79 of the GDPR, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules which are set forth in *Articles 19 and 21 of the BCRs;*

f) the acceptance by the controller or processor established on the territory of a Member State of its liability for any breaches of the binding corporate rules by any member concerned not established in the Union as well as the exemption from that liability, in whole or in part, only if the concerned party proves that that member is not responsible for the event giving rise to the damage are specified in *Article 23 of the BCRs;*

g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of Article 47.2 of the

GDPR are provided to the data subjects in addition to Articles 13 and 14 of the GDPR, is specified in *Article 27 of the BCRs;*

h) the tasks of any data protection officer designated in accordance with Article 37 of the GDPR or any other person or entity in charge of monitoring the compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling are detailed in *Article 26 of the BCRs;*

i) the complaint procedures are specified in *Article 21 of the BCRs;*

j) the mechanisms put in place within the group of undertakings for ensuring the monitoring of compliance with the binding corporate rules are detailed in *Article 26 of the BCRs*. Such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. The results of such monitoring are communicated to the person or the entity referred to in point (h) above and to the board of the controlling undertaking of the group of undertakings (in this situation to **ABN AMRO Bank N.V.,** as well as to the data privacy organization) and are available upon request to the competent supervisory authority;

k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authorities are specified in *Article 27 of the BCRs*;

l) the cooperation mechanism put in place with the supervisory authority to ensure compliance by any member of the group of undertakings is specified in *Article 24 of the BCRs*. The obligation to make available to the supervisory authority the results of the monitoring of the measures referred to in point (j) above is specified in *Article 26.6 of the BCRs;*

m) the mechanisms for reporting, upon request, to the competent supervisory authority any legal requirements to which a member of the group of undertakings is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules are described in *Articles 16 and 17 of the BCRs*;

n) finally, provide for an appropriate data protection training to personnel having permanent or regular access to personal data (*Article 26 of the BCRs*).

7. The EDPB provided its **Opinion 6/2026** in accordance with Article 64(1)(f) of the GDPR.

DECIDES AS FOLLOWING:

1. The Autoriteit Persoonsgegevens approves the Controller BCRs of **ABN AMRO Bank** as providing appropriate safeguards for the transfer of personal data in accordance with Article 46(1) and (2) (b) and Article 47(1) and (2) GDPR. For the avoidance of doubt, the Autoriteit Persoonsgegevens recalls that the approval of BCRs does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

2. The approved BCRs will not require any specific authorization from the concerned SAs.

3. In accordance with Article 58(2)(j) GDPR, each concerned SA maintains the power to order the suspension of data flows to a recipient in a third country or to an international organization whenever the appropriate safeguards envisaged by the Controller BCRs of **ABN AMRO Bank** are not respected.

4. **Annex 1** forms an integral part of this decision and shall be considered a binding appendix thereto.

5. **Annex 2** contains the Controller BCRs which are approved by this decision, and forms an integral part of this decision.

The Hague, 02-03-2026
Yours sincerely,

Autoriteit Persoonsgegevens

Chair

Legal remedy

If you do not agree with this decision, you can submit a notice of objection.[2] The notice of objection must be signed and dated, include the name and address of the (legal) person submitting it and should entail a description of the decision against which the objection is being lodged and the grounds on which it is based. The notice of objection must be received by the Autoriteit Persoonsgegevens within six weeks after this decision is taken. Please address the notice to the Autoriteit Persoonsgegevens and submit the notice via PO Box 93374, 2509 AJ The Hague, The Netherlands.[3]

It is also possible to submit a notice of objection via our web form on the website, see https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/bezwaar-maken .

Please note that submitting a notice of objection will not automatically suspend the effect of this decision.

[2] The Dutch General Administrative Law Act ("Algemene wet bestuursrecht') applies to this procedure.
[3] Article 6:7 in conjunction with article 6:8 (1) of the Dutch General Administrative Law Act.

ANNEX 1 TO THE DECISION

The Controller BCRs of **ABN AMRO Bank** that are hereby approved cover the following:

a. **Scope.**
Article 3.1 of the BCRs:
These BCR's apply if an ABN AMRO Group Company subject to the GDPR Transfers Personal Data (the 'ABN AMRO Data Exporter') to an ABN AMRO Group Company receiving and Processing the Personal Data in a Non-Adequate Country, irrespective of whether or not this receiving ABN AMRO Group Company is subject to the GDPR (the 'ABN AMRO Data Importer'). For completeness' sake, Transfers to ABN AMRO Data Importers in an Adequate Country are not in scope of these BCR's, as they require no further Transfer mechanism.

b. **EEA countries from which transfers are to be made:**
The Netherlands, Germany, Belgium, France, Greece and Norway

c. **Third countries to which transfers are to be made:**
Australia, Brazil, China, Japan, Singapore, the United Kingdom, and the United States

d. **Purposes of the transfer:**
The purposes are detailed in *Annex B to the BCRs.*
They include the following:

Clients and Client lifecycle management:
- *Client identification and onboarding*
- *Transaction and Market abuse monitoring*
- *Client lifecycle management*
- *Client relationship management (including marketing and record management)*
- *Client support*
- *Service provision, including banking, financing, market access and clearing services*

Employee data:
- *Onboarding, Performance and evaluation of employees*
- *Travel and expense management and relocation services*
- *Talent management and rewards*
- *Payroll management, social benefits, salary payment, pensions, insurance*

General management and governance:
- *Procurement and IT management, internal directory and employee user access and account management*
- *General management, reporting and complying with requests from supervisory authorities, disciplinary actions and litigation*

- *Risk management activities*
- *Security, control, regulatory compliance, whistleblowing, prevention and detection of data loss and fraud*

e. Categories of data subjects concerned by the transfer:

- *Prospects, Clients and client representatives, UBOs, directors, representatives, traders, data subjects that call Client support,*
- *Employees*
- *Other Third parties*

Those categories are specified in *Annex B to the BCRs*.

f. Categories of personal data transferred:

Clients and Client lifecycle management:

- *Client identification and onboarding: Identification data (e.g. name, email address, phone number, identification data including ID, IBAN/BIC, client internal identification number, trader ID, client representatives and director contact information, address of headquarters, chamber of commerce number), Client and service related Information (e.g. contact preferences, client contact and representative contact details, service interests, services requested, financial situation relating to requested services, opt in/opt out, contract(s) and contract details, work permit (where relevant), client information)*
- *Transaction and Market abuse monitoring: Identification data (e.g. name,, email address, phone number, client internal identification number, trader ID, client representatives and director information), Client and service related information (e.g. transaction data and historic transaction data, generated alerts, client orders, contact details and records including voice recordings and transcripts, logs of use of ABN AMRO IT systems and applications)*
- *Client lifecycle management: Identification data (e.g. name, email address, phone number, identification data including ID, IBAN/BIC, client internal identification number, trader ID, client representatives and director contact information, address of headquarters, chamber of commerce number), Client and service related information (e.g. contract and contract details, offers to the client, client preferences and interest, transactions and transaction history, logs of use of ABN AMRO IT systems and applications, client financial situation and credit score, information about employees involved in client lifecycle management)*
- *Client relationship management (including marketing and record management): Identification data (e.g. name, email address, phone number, IBAN/BIC, client internal identification number, client representatives and director information), Client and service related information (e.g. opt in/opt out for newsletters, client interests and preferences, logs of use of ABN AMRO IT systems, applications and website visits including cookie settings and historic contact information, information about employees involved in client relationship management)*

- *Client support: Identification data (e.g. name, phone number, IBAN/BIC, client internal identification number, employee internal identification number, account number), Client and service related information (e.g. information regarding requests to ABN AMRO and answers provided, client survey information, information on complaints and inquiries handling, voice recordings, transcripts of calls, logs of use of ABN AMRO IT systems and applications, information about employees involved in client support)*
- *Service provision, including banking, financing, market access and clearing services: Identification data (e.g. name, phone number, email address, IBAN/BIC, client internal identification number, employee internal identification number, contact details of a regulatory body to report trading activities on behalf of the client as a service), Client and service related information (e.g. contract and contract details, specific service requests or provisions such as reporting trading activities to a regulatory body on request of a client, logs of use of ABN AMRO IT systems and applications, equipment an software information)*

<u>Employee data:</u>

- *Onboarding, Performance and evaluation of employees: Identification data (e.g. name, phone number, email address, identification data including ID, contact persons, job title, (hiring) line manager, employee internal identification number), Professional data (e.g. job application information, CV, diplomas and information regarding training, background check results, information on evaluation including dates and identities of the evaluators, obtained results, assessment of professional skills and competencies, voice recordings for training purposes, wishes as expressed by the employee, career development forecast, salary and salary growth expectations)*
- *Travel and expense management and relocation services: Identification data (e.g. name, employee internal identification number, address, travel locations, temporary residence, email address), Professional data (e.g. employee internal identification number, dates of travel, reason for travel, booking reservations, expenses report, credit card expenses, line reporting manager, IBAN/BIC, previous experiences, foreign languages spoken, working permit (where relevant), employees wishes regarding expatriation, data regarding visa)*
- *Talent management and rewards: Identification data (e.g. name, Job title, employee internal identification number, email address), Professional data (e.g. foreign languages spoken, CV, previous experience, working location, function title, development forecast, salary information, assessment of knowledge and trainings and diplomas)*
- *Payroll management, social benefits, salary payment, pensions, insurance: Identification data (e.g. name, address, IBAN/BIC, salary wages, employee internal identification number, social security number, family status, bank account number), Professional data (e.g. employee internal identification number, information regarding cost reimbursement, contract type, hours of work and work schedule, work overtime, absences including sick leaves, unpaid leave, vacations)*

<u>General management and governance:</u>

- *Procurement and IT management, internal directory and employee user access and account management: Identification data (e.g. name, email address, phone number, employee internal identification number, job title, line manager, team members), Professional and technical data (e.g.*

office location, user account information, employee internal identification number, access rights, device ID information, technical connection data, login data, IP address, user account information, information relating to monitoring information embedded in and use of applications),(external) client support contact details, information regarding physical location for facility and access management purposes)

- *General management, reporting and complying with requests from supervisory authorities, disciplinary actions and litigation: Identification information (e.g. name, email address, phone number, client internal identification number, employee internal identification number, contact information relating to third parties, including business partners, counterparties, law firms, accountancy firms, suppliers, contacts at supervisory authorities, contact details of ABN AMRO group management/global management team, shareholder information), Professional data (e.g. job titles, line manager, office location, delegation of authorities, proxy information, line manager, logs of use of ABN AMRO IT systems and applications, information relating to (potential) disciplinary actions, client or employee related investigations or litigation information, information on previous contacts with ABN AMRO, information on voting rights)*
- *Risk management activities: Identification data (e.g. name, email address, phone number, client internal identification number, employee internal identification number, client representatives and business contact details, including directors, UBOs and representatives, proxy information, contact details of third parties including contact details of supervisory authorities), Professional and business operational information (e.g. client relationship contract, transaction information, order and trading activities, office location, line manager, job title, IP address, technical connection data, user account information, access rights), Operational risk management and incident related information (e.g. operational and credit risks information relating to clients, estimated operational risks, incidents reported, login data, user account information, information regarding (potential) disciplinary actions, logs of use of ABN AMRO IT systems and applications, outcome of investigations and follow-up)*
- *Security, control, regulatory compliance, whistleblowing, prevention and detection of data loss and fraud: Identification data (e.g. name, email address, phone number, employee internal identification number, client internal identification number, bank account number, contact details of supervisory authorities), Professional and technical data (e.g. contract type, internal employee identification number, internal client identification number, proxy information, IP address, technical connection data, login data, user account information, access rights, device ID information, device used, logs of use of ABN AMRO IT systems and applications), Incidents and alert information (e.g. incidents and facts reported, evidence, outcome of investigations and follow-up, relation to the person reporting the incident, the person(s implicated in the incident and the person(s) involved in the investigation)*

Those categories are specified in *Annex B to the BCRs.*

Datum
02 March 2026

Ons kenmerk
2023-300387

ANNEX 2 TO THE DECISION

Copy of the Controller BCRs of **ABN AMRO Bank**.