



Rabobank



Rabobank in Ireland

Employee Data Protection Policy

It is the policy of Rabobank Ireland plc, ACC Loan Management Limited and Rabobank International Dublin Branch (including RaboDirect) (“Rabobank”) to comply with their legal obligations relating to the collection, processing, use and storage of personal data of their customers, employees and applicants for employment. Rabobank treats such personal data in accordance with the data protection and other laws of the country in which the data is collected and in particular in accordance with its obligations under the Data Protection Acts 1988-2003 (“the Acts”).

This policy will explain what type of staff personal data is collected and processed, how such personal data is used, and what steps an individual may take to access his or her own personal data. Personal data is as defined in the Acts.

Collection of Employee Data

Rabobank collects certain personal data about its employees, which includes but is not exclusive to data such as name and personal details, contact details including next of kin, current and historical job and employment details, total remuneration inclusive of all benefits and payroll deductions, education background, skills and training, performance management information, career and talent management and attendance and absence records. In addition, employees who have personal mortgages with the bank will require personal details to be kept for the purpose of deducting monthly mortgage payments. Should employees be travelling as part of their employment this may require certain details to be provided to a third party for the purposes of making hotel & flight reservations or should employees have company cars personal details will be requested including driving history and penalty points.

Rabobank does not collect personal data that is prohibited by local law.

Safety & Security of Employee Data

Personal data is protected by security safeguards appropriate to the sensitivity of the information such as encryption, password protection, contractual confidentiality and data protection obligations such as restricted and recorded access, as applicable.

Specifically, personal data which may be considered “sensitive” under applicable law that Rabobank may collect and transfer, but only if legally permissible and properly safeguarded, includes:

- Race or ethnic origin, only if so required for government reporting in the individual’s country of residence on such matters as diversity or employment equity,
- Data in relation to the commission or alleged commission of any offence by an employee, or any proceedings for an offence committed or alleged to have been committed by the employee, the disposal of such proceedings or the sentence of any court in such proceedings,
- Data relating to the physical or mental health or condition of the employee as necessary for participation in benefits plans and leaves of absence,
- Union membership for the purpose of deducting membership subscriptions by the Payroll Department.

Use of Employee Data

Rabobank uses personal data for statistical reporting purposes and in order to comply with laws and regulations for a number of employment related purposes which may generally be described as fulfilling its obligations under employment and personal service contracts, managing and administering payrolls and benefit plans, training employees, tracking applicants for employment and their suitability for particular positions; monitoring or facilitating an employee's performance, career, or professional development, managing Rabobank businesses, including budgeting, staffing and resource allocation and complying with legal and regulatory obligations.

Personal details are maintained on the local HR systems and uploaded to a global employee database on a monthly basis. This database holds personal data for all Rabobank employees globally. Access to such data is limited to local Human Resources and the Group Human Resources Programmes (GHRP) team who are based in London & Utrecht. The GHRP team may be required to report employee personal details to Rabobank Group, MBRI / Executive Board on request.

Personal data of employees (i.e. names and date of birth) are screened against EU and US financial sanctions lists as per Rabobank Group policy and under the European and Irish legislation. For more detail on sanctions please visit the Rabobank Sanctions Desk. (<http://sharepoint2007.eu.rabonet.com/sites/compliance/Sanctions%20Desk/default.aspx>)

Personal data of certain employees may be obtained and retained to ensure ongoing compliance with insider trading and money laundering laws (any such data required by the Bank will be directly requested from the relevant employees)

Rabobank will retain certain relevant data where required on cessation of employment, for instance, in relation to pensions and for the purposes of issuing statements of employment

Processing of Employee Data

As an international organisation with individual business units that operate across international borders, to effect employment related functions described above and for improved quality control, timeliness, accuracy and organizational flexibility, Rabobank requires uniform data platforms that can process personal data from around each of its international offices.

All such transfers will be done pursuant to applicable Data Protection law. Rabobank will ensure that all transfers of personal data internationally will be done in such a way that the Rabobank systems have appropriate protections built in to satisfy the various privacy and data protections requirements in the various countries in which Rabobank does business. In particular, Rabobank will ensure that appropriate security measures are included to ensure that access is restricted to only those people with a specific need for the particular information.

All such processing of data is completed within the European Economic Area (EEA) and is in compliance with Irish and European Data Protection legislation.

Disclosure of Employee Data

Disclosure of personal data is limited. Only Rabobank's authorised officers, directors, employees, agents and consultants who have a legitimate reason related to the functions described above are granted access to personal data, and that access is limited to the amount and nature of such data that is necessary to carry out the designated function.

Generally, only certain individuals have access to certain personal data about Rabobank employees, including individuals in the direct line of management who execute managerial responsibilities vis-à-vis an employee, in finance and control who administer payroll process or taxation returns, in human resources who administer the terms and conditions of employment or who make decisions with respect to staffing and resource allocation.

Other individuals with access to personal data may include systems support staff performing their job duties and individuals who need access for legal, tax, accounting, internal audit, regulation compliance or corporate governance purposes.

Right of Access to Personal Data

Individuals have the right of access to a copy of their own personal data held by Rabobank. Such a request in accordance with the provisions of Data Protection Law in Ireland must be made in writing and sent to the Privacy Officer/Compliance Department. The Privacy Officer may require the employee to specify the categories of employee data to which they are seeking access etc. The Privacy officer will revert to the employee within four weeks. The employee may file a complaint to the Chief Privacy Officer of Rabobank Nederland if the Privacy Officer has not responded within one month or the resolution of their request is unsatisfactory.

Personal data is to be maintained as accurately, completely and as up-to-date as is necessary for the purposes for which it is used. Employees are responsible for using self-service and other capabilities that may be available to them to keep personal data up-to-date or to otherwise keep Human Resources notified of any changes to personal data. All individuals have the right to have any incorrect or inaccurate personal data rectified.

For specific information about accessing and/or correcting their personal information, employees should contact the Privacy Officer, Compliance Department.

Automated Individual Decisions

Under Data Protection law where automated decisions are made in relation to an individual there must be a non-automated element (examples detailed in the legislation of such decisions could be decisions relating to an individuals' performance at work, reliability or conduct)

In Rabobank employees are not subject to decisions based solely on the automated processing of data unless such action is required or authorized under applicable law and/or appropriate measures are taken to safeguard legitimate interests such as providing an the opportunity to explain or address any issues.

Complaints Procedure

Employees may file a complaint regarding compliance with this policy or violation of their rights under data protection legislation with the Privacy Officer, Compliance Department. If you have a complaint, in the first instance please contact your Manager.

If your complaint is not resolved, please fill in the Form Privacy Complaint Employee (see Appendix A) and submit it to your Local Privacy Officer. You should email the form for the Local Privacy Officer's attention to fm.ie.acc.compliance from your own Rabobank e-mail account. The Privacy Officer will revert back to you within four weeks.

If the Privacy Officer has not responded within one month or their resolution is unsatisfactory. You may file a complaint with the Chief Privacy Officer of Rabobank Group (fm.rn.dt.privacy@intern.rabobank.nl).

RABOBANK IRELAND DATA PROTECTION POLICY NEW EMPLOYEE SIGN-OFF

By signing below you are confirming that you have read and understood the Rabobank Ireland Data Protection Policy and you agree to the collection, use, processing and transfer of your personal data as described in the above policy.

As outlined in the policy you have the right of access to a copy of your own personal data held by Rabobank and to have any incorrect or inaccurate personal data rectified.

Employee Signature:

Date

Employee Name (please print)

Appendix A
Form Privacy Complaint Employee
(Employee Privacy Code article 16)

Contact details complainant (to be filled in by complainant)

Surname	
First Name	
Department	
Telephone number	
E-mail (Rabobank)	
Employee number (shown on payslip)	

Subject: Complaint in respect of the handling of my employee personal data by Rabobank
<specify><department>

Question / Remark / Complaint:

Procedure

Please send the Form by e-mail (from your own Rabobank e-mail account) to the Local Privacy Officer, mailbox fm.ie.acc.compliance.

The Privacy Officer shall inform you within four weeks of receiving your complaint about how your complaint will be handled.

If the response does not lead to an acceptable solution or is in your opinion otherwise inadequate, you may contact the Chief Privacy Officer of the Rabobank Group at:

fm.rn.dt.privacy@intern.rabobank.nl.