BASF Ireland Limited
Pension & Life Assurance Scheme

Data Protection Policy

Contents

Published: **January 2025**

Executive Summary

The Trustees act as Controller and process personal data (which may be held on paper, electronically, or otherwise) about members and beneficiaries. Data is also processed on the Trustee's behalf by the Processor for the purpose of administration in accordance with its Trust Deed and they also have responsibility for their own actions.

The Trustees recognise the need to treat personal data in an appropriate and lawful manner, in accordance with GDPR. The purpose of this policy is to set out how the Trustees will comply with the GDPR in its capacity as Data Controller.

The Trustees are committed to fulfilling its obligations under the GDPR in respect of all Personal Data held both in manual records and on computer systems. These procedures ensure that the Trustees meet all their obligations.

Glossary

Controller means any Data Controller of the Scheme data (as defined by GDPR)
GDPR means the General Data Protection Regulation
Policy means this Data Protection Policy
Processor means any Data Processor appointed by the Trustees (as defined by GDPR)
Providers means any professional adviser or service provider appointed by the Trustees
Scheme means the BASF Ireland Limited Pension & Life Assurance Scheme
Sponsor means BASF Ireland DAC
Trust Deed means the Definitive Trust Deed and Rules of the Scheme dated 12 July 2010 (as amended)
Trustees means the Trustees of the Scheme from time-to-time

Purpose

This Policy ensures that the Trustees:

- Comply with data protection law and follows good practice
- Protect the rights of its members
- Are open about how it stores and processes member data
- Protect themselves and members from the risks of a data breach

GDPR Application

The GDPR applies to Controllers and Processors.

A Controller determines the purposes and means of processing personal data and a Processor is responsible for processing personal data on behalf of a Controller.

The Trustees as controllers are responsible for the processing of personal data and the processing that is done on its behalf by processors, who will also have their own GDPR responsibilities. Where a Controller uses a Processor, a contractual agreement will also need to be entered into to ensure compliance with GDPR.

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal activities.

Published: **January 2025**

GDPR Requirements

GDPR sets out the key principles, rights and obligations (rules) on the way in which certain types of data can be processed by controllers and processers. The intention and aim of GDPR, and the supporting Data Protection Act, is to ensure that data is kept secure.

The GDPR applies to the processing of personal data that is:

- Wholly or partly by automated means; or
- The processing other than by automated means of personal data which forms part of, or is intended to form part of, a filing system

Defining Personal Data

Personal data only includes information relating to natural persons who:

- Can be identified or who are identifiable, directly from the information in question; or
- Can be indirectly identified from that information in combination with other information

This will include:

- Names of individuals
- Contact addresses, email addresses, and telephone numbers
- Family information in relation to nominated beneficiaries of a member's pension benefits
- Any other personal information relating to members such as date of birth, age, gender, marital status, nationality, Social Security number, bank account details, PAYE and remuneration information, periods of service, membership category and benefit details.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered more sensitive and may only be processed in limited circumstances.

Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. If personal data can be truly anonymised, then the anonymised data is not subject to the GDPR. It is important to understand what personal data is, to understand if the data has been anonymised.

Information about a deceased person does not constitute personal data and is not subject to the GDPR.

Information about trustee directors where they are individually identifiable, and the information relates to them as an individual may constitute personal data.

Other Key Terms

Special Category Data means personal data relating to a person's racial or ethnic origin; political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, sex life and sexual orientation, genetic or biometric data (used for ID purposes).

Processing means operations performed on personal data, including obtaining, recording or storing it, and organising, amending, accessing, using, disclosing, deleting or destroying it.

Joint Data Controller means a person will be a joint data controller where it and one or more other controllers jointly determine the purposes and means of processing.

Published: **January 2025**

Data Protection Principles

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes
- Adequate, relevant and limited to what is necessary
- Accurate, and where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensure appropriate security of the personal data

This Policy sets out how the Trustees will comply with those principles and will ensure that its advisers and service providers do so.

Legal Basis for Processing

The Trustees will process personal data to administer the Scheme and calculate and pay benefits to its members and has concluded that it has a legitimate interest in the holding, processing and retaining of member data for that purpose.

The Trustees also process personal data where the processing is necessary for the Trustees to comply with their legal obligations, for example, when deducting tax from benefits and providing information to the Pensions Authority and calculating and paying benefits in accordance with members' legal rights.

The Trustees will only process "sensitive personal data" about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions, where a further condition is also met. Usually this will mean that the member has given explicit consent.

Use of Personal Data

The Trustees will process data about members for the purpose of administration and to enable the Trustees to meet their legal obligations, for example, the ways that information is used include:

- Identifying members and their survivors and making sure their details are up to date
- Communicating with member and beneficiaries
- Calculating and paying benefits in connection with a member's entitlement
- Making decisions of fact and exercising discretions

From time-to-time the Trustees may process personal data for purposes which relate to the Scheme, but which are not directly necessary for the administration of members' benefits. For example, the Sponsor may request assistance from the Trustees in a project such as an enhanced transfer value offer or to obtain quotations from insurance companies. The Trustees will consider whether they need to carry out a legitimate interest assessment before agreeing to process personal data for such purposes.

The Trustees may process sensitive personal data relating to members including, as appropriate:

- information about a member's physical or mental health in relation to ill health benefits; or
- to comply with legal requirements and obligations to third parties

Processing for Limited Purposes

The Trustees will only process personal data for specific purposes or purposes notified to a member or those specifically permitted by the GDPR.

Data Retention

The Trustees will not keep personal data for longer than is necessary for the purpose.

Accurate Data

The Trustee will take reasonable steps in conjunction with the administrator to keep the personal data it stores about members accurate and up to date. Data that is inaccurate or out of date will be corrected, updated or destroyed as appropriate.

Members should contact the administrator if their personal details change or if they become aware of any inaccuracies in the personal data the Trustees hold.

Adequate, Relevant, and Limited to what is Necessary

The Trustees will hold adequate, relevant, and limited personal data about individuals necessary.

Members' Rights

Members are granted numerous rights in respect of their personal data, including the right to access, erase, or correct their data. As a Controller, the Trustees must facilitate the exercise of data subjects' rights.

Members have the right to:

- Request access to any personal data the Trustees hold about them
- Ask to have inaccurate data held about themselves amended
- Prevent processing that is likely to cause unwarranted substantial damage or distress

If the Trustees hold personal data because it has a legitimate interest in doing so (and not to comply with a legal obligation), the data subject may also have the right to:

- Object to any decision that significantly affects them, being taken solely by a computer or other automated process
- Be forgotten and have their data erased subject to the rights of the Trustees to retain that data

Data Security

The Trustees will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Trustees have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. It will only transfer personal data to a third party if the third party agrees to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

Sharing Data with Third Parties

The Trustees need to engage a range of professional advisers and third parties and to share member personal data with them. The Trustees are obligated to share personal data with certain regulatory authorities.

The Trustees will not normally disclose personal data to a third party without the member's consent unless the Trustees are satisfied that there is a legitimate interest in sharing the data or the third party operates a key component or function. The most common third party that the Trustees will share personal data with is the Administrator, who act as Processor. The Trustees may also share personal data with a joint data controller, such as the Actuary.

GDPR obliges controllers like the Trustees to ensure that there are contracts in place with processors like the administrator that cover certain minimum requirements.

Where the Trustee does disclose personal data to a third party, it will adhere to the data protection principles.

Published: January 2025

Subject Access Requests

Members can ask what personal data is held about them. See the FAQ section for more information.

Data Protection Officer (DPO)

The Trustees have determined that it is not required to appoint a DPO. If circumstances or regulatory requirements change, the Trustees will review this decision with their legal advisers.

Data Protection Impact Assessments (DPIAs)

The Trustees do not consider that the type of processing that it carries out on a day-to-day basis is likely to result in a high risk to the rights and freedoms of the data subjects, with two exceptions; the Trustees consideration of special category data when determining benefit entitlements (e.g. ill-health benefits or the distribution of death benefits), and the processing of a contingent beneficiary's data under an expression of wish form (where the beneficiary is elderly or a minor).

The Trustees have concluded that it is not required to carry out a DPIA in respect of this processing, as they have already completed an informal risk assessment of its existing processing.

Where a new project or way of working, or proposed changes to an existing project or way of working, may involve intensive or higher risk processing of personal data or sensitive personal data, the Trustee will consider whether a DPIA should be carried out.

Training and guidance

The Trustees have received training on its obligations under GDPR. Training needs will be kept under review and refreshed as required. All new Trustees will be required to undertake specific training on the GDPR and data protection requirements.

All Trustees will be required to comply with this Policy.

Breaches of this policy

If a person considers that this policy has not been followed, they should raise the matter with the GDPR Response Team via basfpensions@basf.com. All Trustees will be informed of the data protection breach.

The team will use the **GDPR Breach Incident Action Plan** and the **Breach Assessment Checklist** to review and resolve and incidents that are reported.

Signed on behalf of the Trustee

James Blackman

James Blackman
UK & Ireland Pension Specialist

Date: 6 January 2025

Signed on behalf of the Trustee

Alison Wilkins

Alison Wilkins
UK & Ireland Pensions Manager

Date: 6 January 2025

Published: January 2025

Data Protection & Retention Periods

Plan Documents

Data Classification	Storage	Protections	Duration Retained
Trust Deed & Rules	SharePoint	Encrypted network	For life of the Scheme *
	Paper	Locked cabinet	
Trustee minutes	SharePoint	Encrypted network	As required **
	Paper	Destroyed	Duration of meeting

Sensitive Personal Data

Data Classification	Storage	Protections	Duration Retained
Electronic Member Data	Electronically	Encrypted network	For life of the Scheme *
Member Correspondence	Electronically	Encrypted network	As required **
	Paper	Confidentially Destroyed	Until converted to electronic
Ill Health Early Retirement Cases	SharePoint	Encrypted network	As required **
	Paper	Confidentially Destroyed	Duration of meeting
Discretion Cases	SharePoint	Encrypted network	As required **
	Paper	Confidentially Destroyed	Duration of meeting
Ill Health Income Protection Cases	SharePoint	Encrypted network	As required **
	Paper	Confidentially Destroyed	Duration of meeting
Trustee Meeting Papers	SharePoint	Encrypted network	As required **
	Paper	Confidentially Destroyed	Duration of meeting

For the life of the Scheme - The reason for holding the data indefinitely enables the Trustees to investigate any enquires relating to member benefits.

****As required - The Trustees will not retain personal data for any longer than is necessary but will not normally delete a beneficiary's personal data during the lifetime of the Scheme unless they are satisfied that the data is no longer needed.***

The Trustees believe it is justified in continuing to hold a beneficiary's data after the liability for their benefits has been discharged, on the basis that the data may be needed to respond to queries or complaints. The data may also be needed in the event that an administrative error is discovered which results in the beneficiary's benefits having to be recalculated, and potentially further amounts being paid, in order to fully discharge the Trustees' liability.

If the Scheme is wound-up, the Trustees will determine how long personal data will be retained having regard to the possibility of queries arising after the winding up is complete.

Published: January 2025

BASF
We create chemistry

Subject Access Requests (SARs)

How are SARs identified?
GDPR does not specify how a request should be made, therefore any personal data request made in writing or verbally should be accepted.

What are individuals entitled to?
- Confirmation that their personal data is being processed
- A copy of their personal data
- Other supplementary information

Where should SARs be directed?
SARs should be referred to the administrator in the first instance (include Data Access Request in the request):

BASF
Aon, Building 5200
Cork Airport Business Park
County Cork, T12 FDN3

myfutureme@aon.ie

How long does the Trustee have to respond to a SAR?
The Trustees will act on the **SAR** within **1 month** of receipt. The Trustees may ask the requestor to provide identification. If ID is required, the response time will not commence until documentation has been received. If a request is complex or multiple requests have been made from the member, the response time may be extended by an additional **2 months**.

How are SARs dealt with?
All **SARs** require that the Trustees can locate and isolate an individual's personal data.

Data subject rights only apply to personal data. Individuals do not have any rights under this Policy to be provided with documents or records that do not contain their personal data, or to control or alter Plan processes that do not use personal data (including those that use anonymised or aggregated data, which cannot be considered personal data).

Do any exceptions exist?
Data subject rights are personal in nature, and the exercise of a subject's right must always be balanced against the parallel rights of other individuals (i.e. other data subjects). The Trustees must consider whether it is appropriate to comply with a request if it would mean disclosing personal data of other data subjects.

In rare circumstances, the Trustees may refuse to act on a request where it is **manifestly unfounded** or excessive. A request may be 'manifestly unfounded' where the object of the request is not permitted under the GDPR, or where it is misconceived.

A **SAR** will generally be excessive only where it is repetitive (e.g. the requester is performing their third access request in a 6-month period). It is unlikely that the scope of a single request will render it excessive, even where it may require a substantial investment of the Trustees' time and resources.

All decisions about whether a request is manifestly unfounded or excessive must be taken by the Trustee Chair.

Are SARs chargeable?
In most cases, the Trustees cannot charge a fee to comply with a **SAR**. However, where the request is excessive or if a member requests further copies of their data, a reasonable fee to cover administrative costs can be charged.

Published: January 2025

GDPR Breach Incident Action Plan

In the case of a data breach, the following action plan will be followed GDPR Response Team, acting on behalf of the Trustee.

Action	Timing
The Response Team will assess the breach including: a) Description of the nature of the incident and when it occurred b) Type of data affected (personal, sensitive) c) Categories and number of members affected, if applicable d) Description of the measures taken or proposed to be taken by the third party to address the incident, if applicable ***'Breach Assessment Checklist'* to be completed**	Within 48 hours
The Response Team will notify the following parties: a) Trustee Board (Chair of Trustee) b) Principal Employer (through Head of HR, UK & Ireland, the BASF Legal Team and the BASF Communications Contact) c) Advisers or service providers of the breach as appropriate d) Plan Lawyer	Within 48 hours
The Response team will liaise with the Plan Lawyer to determine the reporting requirements & timeframes for reporting to the **Office of the Information Commissioner (OIC)**. A record should be kept of all breaches whether reported or not. Reports are submitted via www.oic.ie	Within 72 hours
If the personal data breach is high risk to the rights and freedom of the individual (s) the response team will report and work with the legal advisor to Inform any "data subjects" (members or others), if applicable. An appropriate letter/communication will be prepared.	Within 6 weeks
Evaluate, review and agree any changes to security/processes & update GDPR Policy as necessary.	Within 6 weeks

Breach Assessment Checklist

The following information should be reported to the Trustee and the Office of the Information Commissioner.

Basic Information			
Name of person and/or organisation notifying breach (actual & potential)			
Date of breach	DD/MM/YYYY	Date breach discovered	DD/MM/YYYY
Date GDPR Response Team notified			DD/MM/YYYY

Initial Assessment (to be completed within 48 hours)			
Summary of facts			
Categories & number of data subjects affected			
Number of personal data records concerned		Is sensitive data involved?	Yes/No
Cause of breach			

Containment & Recovery (to be undertaken following initial assessment)			
Notify the relevant advisers			
Is the breach ongoing?	Yes/No	Should the breach be reported to the OIC, police or other authority?	Yes/No
What steps can be taken to stop or minimise further issues?			
What steps can be taken to recover the data?			

Detailed Assessment	
What type of data is involved / how sensitive is it?	
Which individuals are affected by the breach?	
What are the likely consequences for the data subjects?	
Where data was lost or stolen, what protections are now in place to secure data?	
What has happened to the data?	
What could the data tell a third party about the data subject?	
Are there are any related breaches or a pattern of similar breaches?	
Are there are wider consequences of the breach?	

Reporting & Communication	
Is this a Personal Data Breach that should be reported to the ICO? Consider: i. Potential harm to the data subject ii. Volume of personal data involved iii. The sensitivity of the data	Yes/No
Does the breach result in a high-risk to the rights and freedoms of an individual data subject such that they should be notified of the breach? Consider: i. The nature of the breach ii. The effect on the individual and potential consequences of the breach iii. Sensitivity of the data iv. Whether there is anything that the data subject can do to mitigate the risk	Yes/No
Does anyone else need to be notified of the breach, e.g. police or the Pensions Authority?	Yes/No

Lessons Learned			
What went wrong?			
What measures could be used to prevent the breach happening again?			
Was the breach reporting process effective?	Yes/No	Does the Risk Register need to be updated?	Yes/No
Was there adequate staff awareness or are there gaps to be filled?			
Are changes needed to the Data Breach or data protection policies?		Yes/No	

Published: **January 2025**