BASF UK Group Pension Scheme

General Data Protection Regulation (GDPR) Compliance Policy

Published: **March 2021**

BASF
We create chemistry

Contents

Published: **March 2021**

BASF UK Group Pension Scheme – Data Protection Policy

Introduction

General Data Protection Regulation (GDPR) applies in the UK from 25 May 2018. It is supplemented in the UK by a Data Protection Act and it is expected to continue to apply regardless of Brexit.

During the course of its activities, BASF Pensions Trustee Limited ('the Trustee') acting as a Data Controller of the BASF UK Group Pension Scheme ('the Scheme') will 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 data processers for the purpose of administering the Scheme in accordance with its trust deed and rules and they will also have responsibility for their own actions.

The Trustee recognises 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 Trustee will comply with the GDPR in its capacity as a Data Controller.

The Trustee is 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 Trustee meets all its obligations.

Purpose

This data protection policy ensures that the Trustee:

- Complies with data protection law and follows good practice
- Protects the rights of its members
- Is open about how it stores and processes member data
- Protects itself and Scheme members from the risks of a data breach

Who does the GDPR apply to?

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 Trustee as a controller is responsible for the processing of personal data it does 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.

What does GDPR require?

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

Published: March 2021

What is '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
- 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, NI 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 in order 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.

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 Trustee 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 Trustee also processes personal data where the processing is necessary for the Trustee to comply with its legal obligations, for example, when deducting tax from benefits and providing information to HM Revenue and Customs and calculating and paying benefits in accordance with members' legal rights.

The Trustee 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 Trustee will process data about members for the purpose of administering the Scheme and to enable the Trustee to meet its legal obligations, for example, the ways we use that information 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 – such as whether to agree to early payment, or how to distribute benefits after a member's death

From time to time the Trustee 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 Principal Employer may request assistance from the Trustee in a project such as an enhanced transfer value offer or to obtain quotations from insurance companies. The Trustee will consider whether it needs to carry out a legitimate interest assessment before agreeing to process personal data for such purposes.

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

Accurate data

The Trustee will take reasonable steps in conjunction with the Scheme administrators 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 Scheme Administrator via basf@buck.com if their personal details change or if they become aware of any inaccuracies in the personal data the Trustee holds, and appropriate reminders will be provided to members.

Data retention

The Trustee will not keep personal data for longer than is necessary for the purpose. Please see ***'Data Protection & Retention Periods'*** for more information.

Published: March 2021

Adequate, relevant and limited to what is necessary

The Trustee will hold adequate, relevant and limited personal data about individuals that is necessary to the ongoing management of the Scheme.

Processing in line with members' rights

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

Members have the right to:

- Request access to any personal data the Trustee holds 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 Trustee holds 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 Trustee to retain that data

Data security

The Trustee 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 Trustee has 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

While administering the Scheme, The Trustee needs to engage a range of professional advisers and third parties and to share member personal data with them. The Trustee is also under an obligation to share Scheme personal data with certain regulatory authorities, such as HM Revenue & Customs and other statutory bodies (such as the Pensions Ombudsman and the Pensions Regulator).

The Trustee will not normally disclose personal data to a third party without the member's consent unless the Trustee is satisfied that there is a legitimate interest in sharing the data or the third party operates a key component or function of the Scheme. The most common third party that the Trustee will share personal data with is the Scheme's administrators and benefit consultants, who is be acting as a data processor, The Trustee may also share personal data with a joint data controller, such as the Scheme actuary.

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

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

Subject Access Requests

If a member wishes to know what personal data the Trustee holds about them this is called a Subject Access Request (**SAR**). Please see ***'Subject Access Requests (SARs) – FAQs'*** for more information.

Published: March 2021

Data Protection Officer (DPO)

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

Data Protection Impact Assessments (DPIAs)

The Trustee does 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 Trustee's 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 Trustee has concluded that it is not required to carry out a DPIA in respect of this processing, as it has already completed an informal risk assessment of its existing processing as part of its preparations for the introduction of the GDPR in May 2018.

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 Trustee has received training on its obligations under the GDPR. Training needs will be kept under review and refreshed as required.

All new Trustee Directors will be required to undertake specific training on the GDPR and data protection requirements.

All Trustee Directors 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 Trustee directors 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: 1 March 2021

Signed on behalf of the Trustee

Alison Wilkins

Alison Wilkins
UK & Ireland Pensions Manager

Date: 1 March 2021

Published: March 2021

Data Protection & Retention Periods

Data Classification	Storage	Protections	Duration Retained
Scheme Documents			
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			
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 Trustee to investigate any enquires relating to member benefits.***

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

The Trustee 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 Trustee's liability.

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

BASF
We create chemistry

Subject Access Requests (SARs) – FAQs

Question	Answer
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?	All **SARs** should be referred to the scheme administrator in the first instance (include ***Data Access Request*** in the request): • Email: basf@buck.com • By phone: (+44) 0330 123 0647 (Monday to Friday, 9am to 5pm) • In writing: BASF, Buck (Bristol), PO Box 319, Mitcheldean, GL14 9BF
How long does the Trustee have to respond to a SAR?	The Trustee will act on the **SAR** within ***1 month*** of receipt. The Trustee 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 Trustee 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 Scheme 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 Trustee 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 Trustee 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 Trustee's time and resource. **All decisions about whether a request is manifestly unfounded or excessive must be taken by the Chair of Trustees.**
Are SARs chargeable?	In most cases, the Trustee 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: **March 2021**

GDPR Breach Incident Action Plan	

In the case of a GDPR 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) BASF Pension Trustee Limited (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) Scheme Lawyer	Within 48 hours
The Response team will liaise with the Scheme Lawyer to determine the reporting requirements & timeframes for reporting to the **ICO**. A record should be kept of all breaches whether reported or not. Reports are submitted via https://ico.org.uk/for-organisations/report-a-breach/	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 (information to be reported to the Trustee & ICO) – Part 1

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 and 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
What steps can be taken to stop or minimise further loss, destruction or unauthorised disclosure of data?	
What steps can be taken to recover the data?	
Should the breach be reported to the Information Commissioner, the police or other authority?	Yes/No
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 has been 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?	

Published: **March 2021**

Breach Assessment Checklist (information to be reported to the Trustee & ICO) – Part 2

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 (e.g. changing passwords)	Yes/No
Does anyone else need to be notified of the breach, e.g. law enforcement agencies or the Pensions Regulator? (This may already have been considered but should be reconsidered with any additional information)	Yes/No
Lessons Learned	
What went wrong? Consider: Inadequate security measures Human error, etc.	
What technical or organisational measures could be put in place to prevent the breach happening again?	
Did the breach reporting process work properly?	Yes/No
Was there adequate staff awareness or are there gaps to be filled?	
Does the Trustee's risk register need to be updated?	Yes/No
Are any changes needed to the Trustee's Data Breach Policy or related data protection policies?	