Data Protection Policy
Version 1.0, 26.04.18

About this policy

This policy sets out how BIL Group Ltd (**we**/**us**/**our**) will process the personal data of our customers, suppliers, employees/workers/contractors and other third parties.

This policy applies to all personal data that we process regardless of the format or media on which the data are stored or who it relates to.

This policy applies to all members of staff (**you**/**your**). You have a crucial role to play in ensuring that we maintain the trust and confidence of the individuals about whom we process personal data (including our own staff), complying with our legal obligations and protecting our reputation. This policy therefore sets out what we expect from you in this regard.

Compliance with this policy [and the Related policies and procedures set out in Schedule 2] is mandatory. Any breach of this policy and any Related policies and procedures may result in disciplinary action.

This policy is a confidential document and should not be shared with any third party unless approved by a board Director or General Manager in advance.

A glossary of the terms used throughout the policy can be found in Schedule 1.

Scope of this policy

The protection of individuals in relation to the processing of personal data is a fundamental human right. While individuals may have a varying degree of concern for the protection of their personal data, we must nevertheless respect their right to have control over their own personal data; regardless of our important legal obligations. If individuals feel that they can trust us as a custodian of their personal data, this will also help us to fulfil our wider business/charitable/public interest objectives.

The GDPR, as supplemented by the DPA 2018, is the main piece of legislation that governs how we collect and process personal data relating to individuals. Failure to comply with this legislation may have severe consequences for us, including potential fines of up to €20 million or 4% of our total worldwide annual turnover (whichever is higher).

All members of staff, across all business departments and divisions must read, understand and comply with this policy when processing personal data in the course of performing their tasks and must observe and comply with all controls, practices, protocols and training to ensure such compliance.

Mark Farrell, Managing Director is responsible for overseeing the implementation and review of this policy and the Related policies and procedures. They can be contacted as follows:

Name	Mark Farrell
Telephone/Ext	01249 823388
Email	mark@bilgroup.co.uk

If you do not feel confident in your knowledge or understanding of this policy, or you have concerns regarding the implementation of this policy, it is important that you raise this issue with your line manager as soon as possible.

You **must always** contact a board Director or General Manager if you:

- wish to process personal data for any purpose and you are unsure whether we have a lawful basis for doing so (see Lawfulness and fairness)
- need to rely on consent and/or require explicit consent (see Consent as a lawful basis for processing)
- need to prepare a fair processing notice (see Transparency)

- are unsure whether to delete, destroy or keep any personal data (see Storage limitation)
- are unsure about what security or other measures you need to take to protect personal data (see Security, integrity and confidentiality)
- know or suspect that there has been a personal data breach (see Reporting personal data breaches)
- are unsure on what basis to transfer personal data outside of the EEA (see Transfers outside the EEA)
- if you need assistance in dealing with the exercise of any rights by data subjects (see Data subject rights and requests)
- if you plan to use personal data for any purposes other than those they were originally collected for (see Purpose limitation)
- if you are considering the processing of personal data in a new or different way, where a DPIA may be necessary (see Accountability and record-keeping)
- if you plan to undertake any activities involving automated processing including profiling or automated decision-making
- if you are unsure of the legal requirements relating to any direct marketing activities (see Direct marketing)
- if you need help with contracts or any other areas in relation to sharing personal data with a third party (see Sharing personal data)

Key principles

The GDPR is based on a set of key principles that we must observe and comply with at all times from the moment we collect personal data to the moment we delete or destroy it.

We must ensure that all personal data are:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness and transparency)
2. Collected only for specified, explicit and legitimate purposes (Purpose limitation)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed (Data minimisation)
4. Accurate and where necessary kept up to date (Accuracy)
5. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage limitation)
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, integrity and confidentiality)

Additionally, we must ensure that:

1. Personal data are not transferred outside of the EEA (which includes the use of any website or application that is hosted on servers located outside of EEA) to a another

country without appropriate safeguards being in place (see Transfers of personal data outside of the EEA)

2. We allow data subjects to exercise their rights in relation to their personal data (see Data subject rights and requests)

The GDPR requires that we are responsible for, and must be able to demonstrate compliance with, all of the above principles.

Lawfulness, fairness and transparency

Lawfulness and fairness

In order to collect and process personal data for any specific purpose, we must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and also have an adverse impact on a data subject. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by us.

Processing personal data will only be lawful where at least one of the following lawful bases applies:

1. The data subject has given their **consent** for one or more specific purposes
2. The processing is necessary for the **performance of a contract** to which the data subject is a party
3. To comply with our **legal obligations**
4. To protect the **vital interests** of the data subject or another person
5. To pursue our **legitimate interests** where those interests are not outweighed by the interests and rights of data subjects

We must identify and document the lawful basis relied upon by us in relation to the processing of personal data for each specific purpose of group of purposes.

Consent as a lawful basis for processing

There is no hierarchy between the lawful bases for processing above, of which a data subject's consent is one. Consent may not be the most appropriate lawful basis depending on the circumstances.

In order for a data subject's consent to be valid and therefore provide a lawful basis for processing, it must be:

- specific (not given in respect of multiple unrelated purposes)
- informed (explained in plain and accessible language)
- unambiguous and given by a clear affirmative action (meaning opt-in: silence, inactivity or pre-ticked boxes will not be sufficient)

- unbundled from any other terms and conditions provided to the data subject
- freely and genuinely given (there must not be any imbalance in the relationship between us and the data subject and consent must not be a condition for the provision of a product or service)

A data subject must be able to withdraw their consent as easily as they gave it.

Once consent has been given, it may need to be refreshed where we wish to process the personal data for a new purpose that is not compatible with the original purpose.

Unless we are able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, for example a signed document) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside of the EEA. Where we need to process special categories of personal data, we will generally rely on another lawful basis that does not require explicit consent; however we must provide the data subject with a fair processing notice explaining such processing.

If we are unable to demonstrate that we have obtained consent in accordance with the above requirements, we will not be able to rely upon such consent.

Transparency

The principle of transparency runs throughout the GDPR and requires us to ensure that any information provided by us to data subjects about how we process their personal data is concise, easily accessible, easy to understand and written in plain language. Where we have not been transparent about how we process personal data, this will call the lawfulness and fairness of the processing into question.

We can demonstrate transparency through providing data subjects with appropriate privacy notices or fair processing notices **before** we collect and process their personal data and at appropriate times throughout the processing of their personal data.
The GDPR sets out a detailed list of information that must be contained in all privacy notices and fair processing notices, including the types of personal data collected; the purposes for which they will be processed; the lawful basis relied upon for such processing (in the case of legitimate interests, we must explain what those interests are); who we may share the personal data with; and, if we intend to transfer personal data outside of the EEA, the mechanism relied upon by us for such transfer (see Transfers of personal data outside of the EEA).

Where we obtain any personal data about a data subject from a third party (for example, marketing databases purchased by list brokers or CVs from recruitment agents) we must check that it was collected by the third party in accordance the GDPR's requirements and on a lawful basis where the sharing of the personal data with us was clearly explained to the data subject.

All privacy notices and fair processing notices should be reviewed by a board Director or General Manager.

You must observe and comply with our Fair processing and privacy notice procedure.

Purpose limitation

We must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to data subjects **before** we collect and process their personal data.

We must ensure that we do not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where we intend to do so, we must inform the data subjects **before** using their personal data for the new purpose and, where the lawful basis relied upon for the original basis was consent, obtain such consent again.

Data minimisation

The personal data that we collect and process must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is to be processed.

You must only process personal data when necessary for the performance of your duties and tasks and not for any other purposes. Accessing personal data that you are not authorised to access, or that you have no reason to access, may result in disciplinary action.

You may only collect personal data as required for the performance of your duties and tasks and should not ask a data subject to provide more personal data than is strictly for the intended purposes.

You must ensure that when personal data is no longer needed for the specific purposes for which it was collected, that it is deleted, destroyed or anonymised.

You must observe and comply with our Data retention and disposal policy.

Accuracy

The personal data that we collect and process must be accurate and, where necessary, kept up-to-date and must be corrected or deleted without delay when we discover, or we are notified, that the data are inaccurate.

You must ensure that you update all relevant records if you become aware that any personal data are inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted or destroyed.

You must observe and comply with our [Data governance/Information management] policy.

Storage limitation

The personal data that we collect and process must not be kept in a form that identifies a data subject for longer than is necessary in relation to the purposes for which it was collected, except in order to comply with any legal, accounting or reporting requirements.

Storing personal data for longer than necessary may increase the severity of a personal data breach and may also lead to increased costs associated with such storage.

We will maintain policies and procedures to ensure that personal data are deleted, destroyed or anonymised after a reasonable period of time following expiry of the purposes for which they were collected in accordance with our Retention and disposal policy.

You must regularly review any personal data processed by you in the performance of your duties and tasks to assess whether the purposes for which the data were collected have expired. Where appropriate, you must take all reasonable steps to delete or destroy any personal data that we no longer require in accordance with such policy.

All privacy notices and fair processing notices must inform data subjects of the period for which their personal data will be stored or how such period will be determined.

You must observe and comply with our Data retention and disposal policy.

Security, integrity and confidentiality

Security of personal data

The personal data that we collect and process must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage and against unauthorised or unlawful processing.

We will develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed by us
- likelihood and severity of the risks of such processing for the rights of data subjects

We will regularly evaluate and test the effectiveness of the measures implemented by us to ensure that they are adequate and effective.

You are responsible for ensuring the security of the personal data processed by you in the performance of your duties and tasks. You must ensure that you follow all procedures that we have put in place to maintain the security of personal data from collection to destruction.

You must ensure that the confidentiality, integrity and availability of personal data is maintained at all times:

- **Confidentiality:** means that only people who need to know and are authorised to process any personal data can access it
- **Integrity:** means that personal data must be accurate and suitable for the intended purposes
- **Availability:** means that those who need to access the personal data for authorised purposes are able to do so

You must ensure that you observe and comply with our Information security policy.

You must not attempt to circumvent any administrative, physical or technical measures we have implemented as doing so may result in disciplinary action and in certain circumstances, may be a criminal offence.

Reporting personal data breaches

In certain circumstances, the GDPR will require us to notify the ICO and potentially data subjects of any personal data breach.

We have put in place appropriate procedures to deal with any personal data breach and will notify the ICO and/or data subjects where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, you must report this to a board Director immediately and take all appropriate steps to preserve evidence relating to the breach.

You must ensure that you observe and comply with our Personal data breach procedure.

Sharing personal data

You are not permitted to share personal data with third parties unless we have agreed to this in advance, this has been communicated to the data subject in a privacy notice or fair processing notice beforehand and, where such third party is processing the personal data on our behalf, we have undertaken appropriate due diligence of such processor and entered into an agreement with them that complies with the GDPR's requirements for such agreements.

The transfer of any personal data to an unauthorised third party would constitute a breach of the Lawfulness, fairness and transparency principle and, where caused by a security breach, would constitute a personal data breach.

In relation to sharing personal data within our group (which includes our subsidiaries), we may only share personal data with another member of staff who has a need to know such information for the performance of their duties and tasks in relation to such processing and provided the transfer complies with the requirements for Transfers of personal data outside of the EEA.

You must observe and comply with our Data sharing policy.

Transfers of personal data outside of the EEA

The GDPR prohibits the transfer of personal data outside of the EEA in order to ensure that personal data are not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a "transfer" of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

We may only transfer personal data outside of the EEA if one of the following conditions applies:

- the European Commission has issued an "adequacy decision" confirming that the country to which we propose transferring the personal data ensures an adequate level of protection for the rights and freedoms of data subjects
- appropriate safeguards are in place such binding corporate rules, standard contractual clauses that have been approved by the European Commission, an approved code of conduct or a certification mechanism which, in each case, can be obtained from a board Director or General Manager.
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks
- the transfer is necessary in order to perform a contract between us and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent
- the transfer is necessary, in limited circumstances, for our legitimate interests

You must ensure that you do not transfer any personal data outside of the EEA except in the circumstances set out above and provided that we have agreed to this in advance.

You must comply with our Data sharing policy.

Data subject rights and requests

The GDPR provides data subjects with a number of rights in relation to their personal data. These include:

- **Right to withdraw of consent:** where the lawful basis relied upon by us is their consent, to withdraw such consent at any time without having to explain why
- **Right to be informed:** the right to be provided with certain information about how we collect and process their personal data (see Transparency)
- **Right of subject access:** the right to receive a copy of the personal data that we hold, including certain information about how we have processed their personal data
- **Right to rectification:** the right to have inaccurate personal data corrected or incomplete dated completed
- **Right to erasure (right to be forgotten):** the right to ask us to delete or destroy their personal data if: the personal data are longer necessary in relation to the purposes for which they were collected; the data subject has withdrawn their consent (where relevant); the data subject has objected to the processing; the processing was unlawful; the personal data have to be deleted to comply with a legal obligation; the personal data were collected by a child under the age of 13, and they have reached the age of 13
- **Right to restrict processing:** the right to ask us to restrict processing if: the data subject believes the personal data are inaccurate; the processing was unlawful and prefers restriction over erasure; the personal data are longer necessary in relation to the purposes for which they were collected but they are required to establish, exercise or defend a legal claim; the data subject has objected to the processing pending confirmation of whether our legitimate grounds for processing override those of the data subject
- **Right to data portability:** in limited circumstances, the right to receive or ask us to transfer to a third party, a copy of their personal data in a structured, commonly-used and machine-readable format
- **Right to object:** the right to object to processing where the lawful basis for processing communicated to the data subject was our legitimate interests and the data subject contests those interests
- **Right to object to direct marketing:** the right to request that we do not process their personal data for direct marketing purposes
- **Right to object to decisions based solely on automated processing (including profiling):** the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention
- **Right to be notified of a personal data breach:** the right to be notified of a personal data breach which is likely to result in a high risk to the data subject's rights or freedoms
- **Right to complain:** the right to make a complaint to the ICO or another appropriate supervisory authority

You must be able to identify when a request has been made and must verify the identity of the individual making a request before complying with it. You should be way of third parties deceiving you into providing personal data relating to a data subject without their authorisation.

You must immediately forward any request made by a data subject (even if you are uncertain whether it represents a request as set out above) to a board Director or General Manager.

You must observe and comply with our Data subject requests procedure.

Accountability and record-keeping

We are responsible for and must be able to demonstrate compliance with the Key principles and our other obligations under the GDPR. This is known as the 'accountability principle'.

We must ensure that we have adequate resources, systems and processes in place to demonstrate compliance with our obligations including:

- where necessary, appointing a suitably qualified and experienced DPO and an executive accountable for data protection
- ensuring that at the time of deciding how we will process personal data and throughout, implementing appropriate technical and organisational measures that are designed to ensure compliance with the Key principles (called 'Data Protection by Design')
- ensuring that, by default, only personal data that are necessary for each specific purposes are processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal data (called 'Data Protection by Default')
- ensuring that where any intended processing presents a high risk to the rights and freedoms of data subjects, that we have carried out an assessment of those risks and taking steps to mitigate those risks (by undertaking a 'Data Protection Impact Assessment'). Please see our Data protection impact assessment policy.
- integrating data protection into our internal documents, privacy notices and fair processing notices
- regularly training our staff on the GDPR, this policy and our Related policies and procedures and maintaining a record of training attendance by members of staff
- regularly testing the measures implemented by us and conducting periodic reviews to assess the adequacy and effectiveness of this policy and our Related policies and procedures

We must keep full and accurate records of all of our processing activities in accordance with the GDPR's requirements.

You must ensure that have undertaken the necessary training providing by us and, where you are responsible for other members of staff, that they have done so.

You must further review all the systems and processes under your control to ensure are adequate and effective for the purposes of facilitating compliance with our obligations and your obligations under this policy.

You must ensure that you observe and comply with our Data governance/Information management policy.

Direct marketing

In addition to our obligations under the GDPR, we are also subject to more specific rules in relation to direct marketing by email, fax, SMS or telephone. We must ensure that when a data subject exercises their right to object to direct marketing, that we have honoured such request promptly.

You must ensure that you understand or consult with Tim Murrow, General Manager on our legal obligations in relation to direct marketing before embarking upon any direct marketing campaign.

You must observe and comply with our Direct marketing policy.

Changes to this policy

We reserve the right to change this policy at any time without notice, so please review this policy regularly to obtain the latest copy.

This policy does not override the GDPR or any other applicable data protection laws and regulations both in the UK or any other country where we operate or process personal data relating to the citizens of any other country.

By signing below, I acknowledge that I have received a copy of the Data Protection Policy (Version 1.0, 26.04.18) and that I have read and understood it.		
Signature	**Name**	**Date**

Schedule 1 – Glossary

automated processing	any form of processing (including profiling) that is undertaken by automated means to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements
consent	any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data about them
controller	the person or organisation that determines the purposes and means of processing personal data
criminal convictions and offences	personal data relating to criminal convictions, the commission or alleged commission of an offence, proceedings for the commission or alleged commission of an offence and sentencing
Data Protection Impact Assessment (DPIA)	a tool used to identify and reduce the risks of a processing activity and which must be undertaken in certain circumstances specified in the GDPR.
data subject	an individual to whom personal data relates and who can be identified or is identifiable from personal data
Data Protection Officer (DPO)	a person required to be appointed in specific circumstances under the GDPR and who must have expert knowledge of data protection law and practice. Where a mandatory DPO has not been appointed, this term means a person that has been delegated responsibility for our compliance with data protection law or a voluntary appointment of a DPO.
[DPA 2018]	the UK Data Protection Act 2018
EEA	the 28 countries in the European Union and Iceland, Lichtenstein and Norway
explicit consent	a higher standard of consent that requires a very clear and specific statement rather than an action which is suggestive of consent
fair processing notices	a notice setting out information that must be provided to data subjects before collecting personal data from them including notices aimed at a specific groups of individuals or notices that are presented to a data subject on a 'just-in-time' basis

GDPR	the General Data Protection Regulation (Regulation (EU) 2016/679)
personal data	any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes criminal convictions and offences data, special categories of personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
personal data breach	a breach of security lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and which compromises the confidentiality, integrity, availability and/or security of the personal data
privacy notices	see fair processing notices above
process, processes, processing	any activity or set of activities which involves personal data including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or making available, alignment or combination, restriction, erasure or destruction
pseudonymised, pseudonymisation	replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the data subject cannot be identified without combining the identifier or pseudonym with other information which has been kept separately and securely. Personal data that have been pseudonymised is still treated as personal data (unlike personal data which has been anonymised)
[Related policies and procedures]	the related policies and procedures listed in Schedule 1 – Glossary
special categories of personal data	previously known as "sensitive personal data" under the Data Protection Act 1998, this means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and, for the purposes of this policy personal data relating to criminal offences and convictions.

staff	our agents, consultants, contractors, directors, employees, representatives, and other representatives

Schedule 2 – Related Policies & Procedures

[List of other related policies and procedures if applicable]