BAY PLASTICS

Bay Plastics

GDPR (GENERAL DATA PROTECTION REGULATIONS) POLICY

REF: GDPR0001

VERSION: 4.0

ISSUE DATE: SEPTEMBER 2024

Contents

1. GDPR (General Data Protection Regulations) Policy

POLICY STATEMENT

Bay Plastics wants to ensure that all employees understand the processes they need to follow to ensure that we all comply with GDPR regulations and laws.

We need to collect and use information about people with whom we work, to allow us to carry out business and provide our services. These may include members of the public, current, past, and prospective employees, clients, customers, and suppliers. In addition, by law, we may be required to collect and use information. All personal information, whether in paper format, electronic, or any other format, must be handled and managed in accordance with GDPR.

GDPR PRINCIPLES

Bay Plastics fully supports and complies with UK GDPR and the six principles of the Data Protection Act. In summary, this means personal information must be:

- Processed fairly and lawfully and in a transparent manner.
- Collected for specified, explicit, and legitimate 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 data is processed.
- Processed in a manner that ensures appropriate security of the personal data.

BAY PLASTICS

2. What is GDPR?

The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the United Kingdom and the European Union (EU).

The GDPR requires Bay Plastics to implement appropriate technical and organisational security measures to protect personal data and processing systems. In the context of the GDPR, our physical and virtual server environments are potentially processing personal and sensitive data.

Adopted in April 2016, the Regulation came into full effect in May 2018, after a two-year transition period.

3. Do I Need to Comply with GDPR?

The simple answer is YES! Whilst Bay Plastics are responsible for ensuring that we have GDPR policies and procedures in place to comply with GDPR, all employees are accountable for compliance with GDPR law and regulations. We must all:

- Process personal data lawfully, fairly, and transparently.
- Only collect data for specified, legitimate purposes and process it for those purposes.
- Limit the collection of personal data to what is needed for the purpose of which it is required.
- Keep all personal data accurate and up to date.
- Only retain personal data for as long as is necessary for the purpose it was collected.
- Process personal data securely and confidentially to ensure it is not misused, lost, hacked, stolen, damaged, or destroyed.

Bay Plastics are responsible for ensuring that we have the following:

- GDPR Policy - This is the policy! This policy sets out how we protect personal data.
- Employee Privacy Notice - See Section 4 of this policy. This explains how we (The Company) process employees personal data.
- Customer Privacy Notice - Promotes transparency and provides individuals with control over what data we hold and how we use it.
- Data Retention Policy - See Section 4 of this policy. This details our protocols for retaining information.
- Data Retention Schedule - Our schedules set out how long we should keep data for and when we should discard this information.
- Data Subject Request Policy & Procedure - See Section 5 of this policy.
- Data Breach Policy & Procedure - See Section 6 of this policy.

4. Privacy Notice (Employees, Workers, Volunteers, Interns & Apprentices

Bay Plastics are a “Data Controller”. This means that we are responsible for deciding how we hold and use personal data. This notice applies to current and former employees, workers, volunteers, interns and apprentices. An employee is someone who works under a contract of employment, whilst a person is generally classed as a worker if they have a contract or other arrangement to do work or services personally for a reward, their reward could be for money or a benefit in kind, for example, the promise of a contract or future work.

Whilst we are required by law to notify you of the information we hold on you, this notice does not form part of any contract of employment. We may update this notice at any time, but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practicable.

It is important that you read this notice (Section 4 of this policy), together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are we using such information, what your rights are under the data protection legislation, and that we will do so in line with the six data protection principles detailed in Section 1 of this document.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependents.
- Next of kin and emergency contact information.
- National insurance number.
- Bank account details, payroll records, and tax status information.
- Salary, annual leave, pension, and benefits information.
- Start date, and if different, the date of your continuous employment.
- Leaving date and your reason for leaving.
- Location of employment or workplace.
- Copy of driving licence and driving records (including telematics).
- Recruitment information (including copies of right to work documentation, references, and other included in a CV or cover letter, or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records, and professional memberships).
- Compensation history.
- Performance information.
- Disciplinary and grievance information.
- Information obtained through electronic means such as swipe card records/biometrics.
- Information about your use of our information and communications systems.
- Photographs.
- Results of HMRC employment status check, details of your interest in and connection with intermediary through which your services are supplied.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation, and political opinions.
- Information about your health, including any medical condition, health and sickness records, including:
- Where you leave employment and the reason for leaving is determined to be ill-health, injury, or disability, the records relating to that decision.
- Details of any absences (other than holidays) from work, including time on statutory parental leave and sick leave, and;
- Where you leave employment and the reason for leaving is related to your health, information about that condition is needed for pension.
- Information about criminal convictions and offences.

HOW IS YOUR PERSONAL INFORMATION COLLECTED?

We collect personal information about employees, workers, volunteers, interns and apprentices through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third employees including former employers.

We may also collect personal information from managers of pension arrangements operated by a group company.

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for legitimate interests pursued by us or a third party, and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following circumstances, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL INFORMATION

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal information to pursue legitimate interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Administering the contract we have entered into with you.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs), and for disclosures we have to make to the HMRC.
- Providing the benefits to you that are part of your contract of employment.
- Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties.
- Liaising with the managers of a pension arrangement operated by a group company, your pension provider, and any other providers of employee benefits.
- Business management and planning, including accounting, auditing, and compliance.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training, and development requirements.
- Dealing with legal disputes involving you, or other employees, workers, volunteers, interns and apprentices, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety, data protection, insurance and driving obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies. This may include retention of emails and phone recordings which can be used for quality checks, training, or in correlation with company policies.

- To ensure network information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics studies to review and better understand employee retention and attrition rates.
- Equal opportunities monitoring.
- In relation to images, for identification and security purposes and, with your consent for engagement, brand promotion and internal communications.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

IF YOU FAIL TO PROVIDE PERSONAL INFORMATION

If you fail to provide certain personal information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Failing to provide information will hinder our ability to administer the rights and obligations arising as a result of the employment relationship effectively.

CHANGE OF PURPOSE

We will only use your personal information for the purposes which we collected it, unless we reasonably consider that we need to use it for another reason that is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

Please note that we may process your personal information without your knowledge or consent, in “special categories” of personal information, such as information about your health, racial or ethnic origin, or sexual orientation. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.
- Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to an occupational pension scheme.
- Where it is needed for the purpose of preventative or occupational health medicine or for the assessment of the working capacity of the employee.

Less commonly, we may process this type of information where it is needed in relation to legal claims, or where it is needed to protect your interests (or someone else’s interests), and you are not capable of giving your consent, or where you have already made the information public.

SITUATIONS IN WHICH WE WILL USE YOUR SENSITIVE PERSONAL INFORMATION

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive information are listed below. We have indicated the purpose or purposes for which we are processing or will process your more sensitive information.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence, and to administer benefits including statutory maternity pay, statutory sick pay, pensions, and permanent health insurance. We need to process this information to exercise rights and perform obligations in connection with your employment.
- We will use information about your race or nationality or ethnic origins, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

DO WE NEED YOUR CONSENT?

We do not need your consent if we use special categories of your personal information in certain circumstances to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- Determine suitability for employment / ongoing employment.

We are allowed to use your personal information in this way to adhere to legislative requirements, for example the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975.

Where a role requires a Disclosure and Barring Service (DBS) check, in order to progress this, we will ask you to provide your details to a company that will administer the DBS checks for us directly with the Disclosure and Barring Service.

DATA SHARING

We may have to share your data with third parties, including our third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

WHY MIGHT YOU SHARE MY PERSONAL INFORMATION WITH THIRD PARTIES?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

WHICH THIRD-PARTY SERVICE PROVIDERS ACCESS MY PERSONAL INFORMATION?

“Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our group. The following third-party service providers process personal information about you for the following purposes:

- Service providers that enable us to have the necessary business solutions to administer the working relationship with you and meet business requirements / corporate objectives e.g., HR database provider.
- Benefit providers to administer the benefits you are entitled to e.g., sickness absence insurance and reward platforms.
- Pension providers for the purposes of operating your participation in any pension arrangement.
- Insurance providers for the purposes of insurance and the administration of claims; and
- The suppliers we work with and provide a service for to meet our contractual arrangements.

HOW SECURE IS MY INFORMATION WITH THIRD-PARTY SERVICE PROVIDERS AND OTHER ENTITIES IN OUR GROUP?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information.

We do not allow our third-party service providers to use your personal information for their own purposes. We only permit them to process your personal information for specified purposes and in accordance with instructions.

WHEN WE MIGHT SHARE YOUR PERSONAL INFORMATION WITH A THIRD-PARTY

We will share your personal information with other entities in our group as part of our regular reporting activities on company performance, in the context of a business reorganisation or group restructuring exercise, for system maintenance support and hosting of data. We will share personal information relating to your pension arrangements operated by a group company with other entities in the group for the purposes of administering the share plans.

WHAT ABOUT OTHER THIRD-PARTIES?

We may share your personal information with other third parties:

- In the context of the possible sale or restructuring of the business. In this situation we will, so far as possible, share anonymised data with the other parties before the transaction completes. Once the transaction is completed, we will share your personal information with the other parties if and to the extent required under the terms of the transaction.
- To comply with any legal, audit or regulatory obligations, or in order to enforce or apply our terms and conditions and other agreements. This includes disclosing personal information in response to a request from law enforcement or other regulatory authorities or sharing for fraud prevention purposes.
- With regulatory authorities, courts and governmental agencies to comply with legal orders, legal or regulatory requirements, government requests and other lawful requests. We may also share your personal information with our legal and other professional advisors.

TRANSFERRING INFORMATION OUTSIDE THE EU

Your personal information may be stored and transferred to locations outside the European Union including countries that may not have the same level of protection for personal information. When we do this, we will ensure it has an appropriate level of protection in accordance with Data Protection Law, and that the transfer is lawful.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, access to your personal information is limited to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION - HOW LONG MAY YOU USE MY INFORMATION?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information, we consider the amount, nature, and sensitivity of the personal information, the potential risk of harm from unauthorised use or disclosure of your personal information, the purposes for which we process your personal information and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with the determined timescales.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION - YOUR DUTY TO INFORM US OF CHANGES

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

If you want to correct your personal information, this should be submitted to the HR department.

YOUR RIGHTS IN CONNECTION WITH PERSONAL INFORMATION

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.

If you want to review, verify or request erasure of your personal information, object to the processing, or request that we transfer a copy of your personal information to another party, you can request this via the HR department. We will respond to a rights request in accordance with data protection legislation

NO FEE USUALLY REQUIRED

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

WHAT WE MAY NEED FROM YOU

We may need to request specific information from you to help us confirm your identity to ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it. You may be asked for further information to locate the personal information before the request can be processed. You will be informed if we require further information to locate the personal information and/ or to verify your identity.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our HR Department. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact our HR Department.

5. Data Subject Request Procedure

PURPOSE

The purpose of this procedure is to set out how Bay Plastics ("the Company"), will deal with requests involving personal data, known as "Data Subject Requests". In particular:

- Ensure good practice in dealing with Data Subject Requests.
- Ensure compliance with the Data Protection Act 2018.
- Ensure compliance with any other applicable legislation and regulation (General Data Protection Regulation 2016) related to personal data.
- Ensure that all responses to Data Subject Requests comply with relevant local and international regulations on data protection and information security; and
- Ensure those responses are in the interest of both the data subject and the Company.

Specifically, where personal data is being processed by the Company and the identity of the data subject has been confirmed, the Company shall respond to the request and provide the data subject with a response.

SCOPE

This procedure applies to all those with authorised access to personal data processed by the Company irrespective of status, including employees, temporary staff, contractors, consultants and suppliers.

It covers all requests involving personal data including, but not limited to:

- Access requests.
- Rectification requests.
- Erasure requests.
- Right to restrict processing.
- Transfer (portability) requests.
- Rights to object to processing, including right to object to receive marketing.

Further information on these rights can be found within Appendix A.

ROLES, RESPONSIBILITIES & INTERPRETATION

All employees have a responsibility to adhere to this procedure regardless of their status.

A checklist of actions can be found within Appendix B and relevant terms defined in Appendix C.

HOW TO RECOGNISE A REQUEST

A request could be received by any Bay Plastics employee or department within the Company and could be made verbally or in writing (email, post, social media etc.). If an employee is unsure of whether they have received a request, they are to contact the HR department for advice, hr@bayplastics.co.uk

WHO CAN MAKE A REQUEST?

The individual the request relates to (data subject), or their nominated representative can make a Data Subject Request.

WHAT SHOULD AN EMPLOYEE DO IF THEY RECEIVE A REQUEST?

An employee who receives a Data Subject Request should pass the following information to the HR department:

- The requestors name.
- Who it relates to (if different)?
- The right they are requesting and what information it relates to (if known) and
- The date the request was received.

IDENTIFICATION

The data subject must prove their identity to any disclosure of any information or to action the majority of requests. This will be a certified photocopy of 2 forms of evidence that prove their identity and address, such as driving licence and utility bill with their name on within the last 6 months. This may be varied dependant on the level of identification required to provide the Company with satisfactory evidence of proof of identity.

Where there are any reasonable doubts concerning the identity of the data subject, additional information must be requested to confirm the identity of the data subject. If the Company is still not in a position to identify the data subject, the data subject shall be informed accordingly, if possible.

There are occasions whereby a data subject may agree to a third party making a request, such as a solicitor, somebody looking after their welfare or potential employer. To protect a data subject's data the Company will make all necessary checks to satisfy it that the individual making the request on behalf of the data subject is entitled to do so. This may include requesting written authority to make the request (e.g., consent from the data subject) or a more general power of attorney. The request will not be progressed until the Company is satisfied.

The Company may feel it appropriate to contact an individual directly to discuss the request, for example, if asked to release health information. On occasions such as this, the data subject will be given an overview of the type of information that will be released and the option to:

- See their personal data first and, upon consent, it will be released to the third party.
- Grant permission for it to be sent directly to the third party; or
- Withdrawn consent and no information will be sent to the third party.

CONTRACTUAL RESPONSIBILITIES

The Company will establish whether the personal data is being processed by the Company acting as a 'Controller' 'Processor' or 'Joint Controller' and ensure it meets its' data protection and

contractual notification obligations with Suppliers, Customers and third parties.

RESPONSE TO ACCESS REQUESTS

Where personal data is being processed by the Company and the data subject makes a request to access the data, the Company shall provide the data subject with access to the personal data and, if requested:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data have been or will be disclosed (where transferred outside the EU, include the appropriate safeguards relating to the transfer)
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request from the Company the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with a supervisory authority where the personal data are not collected from the data subject, any available information as to their source.
- Any existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and
- Where personal data are transferred to a third country or to an international organisation, the appropriate safeguards relating to the transfer.

RESPONSE TO RECTIFICATION REQUESTS

Where a Data Subject Request is for the rectification of inaccurate personal data, the Company shall carry this out without undue delay where the request does not conflict with any legal, regulatory or other such constraints. This may include updating personal data by means of a supplementary statement.

The Company shall inform any third parties who have been sent personal data that the data subject has made a rectification request and instruct all parties what rectification is required.

RESPONSE TO ERASURE REQUESTS

When requested to do so by the data subject, the Company will erase personal data without undue delay where the request does not conflict with any legal, regulatory or other such constraints.

The majority of personal data the Company collects, uses and stores is for the purposes of the performance of a contract with an individual, for the legitimate purposes to manage a business and employment relationship and to meet legal obligations.

Therefore, it is unlikely the Company will be able to erase personal data prior to its planned destruction date as it would be required for compliance with legal obligations and to establish, exercise or defend any legal claims. Decisions will be made on a case-by-case basis.

The Company shall instruct third parties that have been sent personal data that the data subject has made a request for erasure (including any third parties holding data that has been made public).

RESPONSE TO OBJECTION AND RESTRICTION REQUESTS

The data subject shall have the right to withdraw his or her consent to their personal data being processed at any time, where the legal basis for processing is based on consent.

Where a data subject objects to the processing of their personal data for a specific purpose, and the lawful basis for processing is based on legitimate interest pursued by the Controller, the Company shall no longer process the personal data for such purposes except where there are any legal, regulatory or other such constraints. The exception to this is where a data subject objects to marketing, this is an absolute right and marketing must cease.

When requested to do so by the data subject, the Company shall restrict the use of their personal data where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the Company to verify the accuracy of the personal data.
- The processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
- The Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.
- Where the data subject has objected to processing and the Company are in the process of verification whether the objection is on legitimate grounds.

A data subject who obtained the restriction of processing shall be informed by the Company before the restriction of processing is lifted.

RESPONSE TO TRANSFER REQUESTS (DATA PORTABILITY)

The Company shall carry out a request from a data subject to transmit personal data to another data controller without hindrance, where:

- The processing of the personal data is based on consent or for the performance of a contract with the data subject.
- The processing of the personal data is carried out by automated means; and
- The request does not conflict with any legal, regulatory or other such constraints.

Transmitted data shall be in a structured, commonly used and machine-readable format, and transmitted securely.

The Company is not responsible for compliance of the receiving organisation with data protection law as it would be acting upon the data subject's request.

RESPONSE FORMAT

The data in any response shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The response shall be provided in the medium requested by the data subject. Where no medium has been specified, the response shall be:

- In writing, for requests received in writing.
- In a commonly used electronic form, for requests received via email; and
- Provided orally, for requests received orally.

RESPONSE TIMES

The HR department shall provide a response to the data subject without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The HR department shall inform the data subject of any extension within one month of receipt of the request, together with the reasons for the delay.

If it is not possible to action the request of the data subject, the Company shall inform the data subject without undue delay and at the latest within one month of receipt of the request of the reasons for not taking action and of the possibility of lodging a complaint to a supervisory authority and seeking a judicial remedy.

No written response will be provided to data subjects who object to marketing over the phone, as these will automatically be given to the data team to suppress details.

FEES

One copy of the personal data shall be provided free of charge. For further copies of the data, the Company shall charge a reasonable fee to the data subject based on administrative costs.

EXCEPTIONS

Where requests from a data subject are manifestly unfounded or excessive, either:

- The data subject should be charged a reasonable fee; or
- The data subject should be informed that the Company will not act on the request and the associated reasons.

Any information sent to the data subject should not include any personal data about (or such that it would allow the data subject to identify) any third party unless permission has been sought and received from that individual, or it is reasonable in all circumstances to release the information without consent. The Company would give regard to The Data Protection Act 2018, The General Data Protection Regulation 2016 and Article 8 of the Human Rights Act 1998.

Where redactions are to take place, care must be taken to ensure that either blanking out third party names/ addresses/identification or providing the information in another format (i.e., typed) does not disclose the identity of a third party.

The Data Protection Act 2018 provides exemptions which enable the Company to disapply data subject rights in certain circumstances. For example, the prevention and detection of a crime (e.g., benefit fraud), disclosure required for legal proceedings / advice (e.g., obtaining legal advice in regard to a claim), negotiations, management forecasts.

Where appropriate, the Company will take into consideration the relevant exemptions and where an exemption is applied the Company is not required to cite the exemption used.

REQUEST LOG

A log of requests and associated documentation is retained to ensure that the Company is able to track the number of requests that it receives and that it is responding in a compliant manner to those requests within the correct timeframe.

COMPLAINTS

If the data subject or their representative is not satisfied with the outcome of their rights request, in the first instance, the individual will be encouraged to attend an informal meeting or have a discussion, with a view to addressing and resolving the issues locally with the HR department or nominated representative.

The data subject can contact the Information Commissioner directly who is the statutory regulator for an assessment on how the Company progressed the request.

INFORMATION SECURITY INCIDENT OR PERSONAL DATA BREACH PROCEDURE

RESPONSIBILITY: All employees have a responsibility to ensure the safe and secure use of information within the company's custody and adhere to this procedure regardless of their status.

DATA BREACH OR SECURITY INCIDENT IS IDENTIFIED -

See Section 6 of the GDPR Policy for more detailed examples of incidents and breaches.

CONTAIN -

Take action to contain the incident or breach.

For example: email recall, secure paper documentation.

REPORT -

Advise your HR department, the Managing Director or a senior manager as soon as the incident / breach is identified.

You should advise of any relevant detail - what, when, how, people involved etc.

MAINTAIN CONFIDENTIALITY -

Do not discuss, share, store or copy information surrounding the incident / breach.

Ensure the General Office Manager is also notified if you believe the incident is a possible IT virus.

NOTIFICATION -

The Data Controller (Managing Director) will make a decision as to whether the ICO (Information Commissioners Office) is to be contated.

This must be done within 72 hours of the incident / breach.

Notification to other parties may also be considered - police, media, third-parties etc.

EVALUATION & RESPONSE -

A follow-up action plan will be developed.

ONGOING RISK ASSESSMENT -

In parallel with the action plan, internal follow up action may be required and external bodies may make suggestions for improvement and / or undertake audits.

Appendix A – Summary of an Individual's Rights

ACCESS REQUESTS

Individuals have the right to find out if an organisation is using or storing their personal data. This is called the right of access. An individual can exercise this right by asking for a copy of their data, which is commonly known as making a 'subject access request'.

Specifically, where personal data is being processed by the Company and the identity of the data subject has been confirmed, the Company shall respond to the request and provide the data subject with a response.

RECTIFICATION REQUESTS

Individuals can challenge the accuracy of personal data held about them by an organisation and ask for it to be corrected or deleted. This is known as the 'right to rectification'. If an

individual's data is incomplete, they can ask for the organisation to complete it by adding more details.

ERASURE REQUESTS

Individuals can ask an organisation that holds data about them to delete that data and, in some circumstances, it must then do so. This is known as the right to erasure. It is sometimes referred to as the 'right to be forgotten'.

RESTRICT PROCESSING

An individual can limit the way an organisation uses their personal data if they are concerned about the accuracy of the data or how it is being used. If necessary, an individual can also stop an organisation deleting their data. Together, these opportunities are known as the 'right to restriction'.

This right is closely linked to an individual's right to challenge the accuracy of their data and object to its use.

TRANSFER (PORTABILITY) REQUESTS

In some circumstances, an individual has the right to get their personal data from an organisation in a way that is accessible and machine-readable, for example as a csv file.

An individual also has the right to ask an organisation to transfer their data to another organisation. An organisation must do this if the transfer is, as the regulation says, "technically feasible".

RIGHT TO OBJECT TO PROCESSING, INCLUDING MARKETING

An individual has the right to object to the processing (use) of their personal data, in some circumstances. If an organisation agrees to an objection, it must stop using the data for that purpose unless it can give strong and legitimate reasons to continue using the data despite an individual's objections.

An individual has an absolute right to object to an organisation using their data for direct marketing (trying to sell things to an individual). This means an organisation must stop using the data for marketing purposes if an individual object.

Appendix B – Data Subject Request Checklist

REQUEST FORWARDING

All employees must forward a personal data request to the HR department for all requests received from a customer or an employee.

EXCEPTIONS

Object to Marketing requests to be sent to the Marketing Manager and rectifications to be dealt with in line with usual procedures.

HR DEPARTMENT - IDENTIFICATION CHECKLIST

Check the identity of the data subject has been verified with acceptable proof of identification, including one of the following:

- Full valid driving licence or.
- Birth certificate or certificate of registry of birth or adoption certificate or.
- Full valid current passport.

AND one of the following:

- Gas, electricity, water or telephone bill in the data subject's name for within the last 6 months.

OR

- Power of attorney / proof of data subject consent etc.
- Confirmed with the employee.

RESPONSE CHECKLIST FOR ALL RESPONSES

Check that:

- The contract with the supplier has been reviewed to determine notification terms.
- The request doesn't conflict with any legal, regulatory or other such constraints (GDPR, DPA, HRA, Employment Law).
- Exceptions / exemptions have been considered where necessary and redactions where appropriate.
- The response has been provided without undue delay and in any event within one month of receipt of the request.
- If a request is not upheld, the reason why and the right to complain to the ICO or request a judicial review.
- The data is presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- The response is in the medium requested by the data subject. Where no medium has been specified, check the response is:
- In writing, for requests received in writing.
- In a commonly used electronic form by secure means, for requests received via email.
- Provided orally, for requests received orally.

RESPONSE CHECKLIST FOR DATA ACCESS REQUESTS

Check the response has included:

- The data requested.
- The purposes of the processing, if requested.
- The categories of personal data concerned, if requested.
- The recipients or categories of recipient to whom the personal data have been or will be disclosed (where transferred outside the EU, include the appropriate safeguards relating to the transfer), if requested.
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period, if requested.
- The existence of the right to request from the Company the rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with a supervisory authority.
- Where the personal data are not collected from the data subject, any available information as to their source, if requested.
- Any existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

RESPONSE CHECKLIST DATA RECTIFICATION REQUESTS

Check the response has included:

- Confirmation that the data has been updated (or added to via a supplementary statement) in all locations in which it resides.
- Confirmation that the all relevant third parties that have been sent the personal data have been informed that the data subject has made a rectification request and what the rectification request was.
- If requested by the data subject inform them of recipients.

RESPONSE CHECKLIST FOR DATA ERASURE REQUESTS

Check the response has included:

- Confirmation that the data has been securely erased in all locations in which it resides.
- Confirmation from all the relevant third parties that have been sent the personal data that they confirm they have been informed by the Company that the data subject has made an erasure request and what the erasure request was.
- If requested by the data subject inform them of recipients.

RESPONSE CHECKLIST FOR DATA OJBECTION AND RESTRICTION REQUESTS

Check the response has included:

- Confirmation that the data processing has been restricted/stopped for that specific purpose.
- Consideration to whether an upheld objection should lead to the erasure (processing) of data.
- Confirmation from all the relevant third parties that have been sent the personal data that they confirm they have been informed by the Company that the data subject has made a restriction request.
- Confirmation that the data subject shall be informed by the Company before the restriction of processing is lifted.
- For restriction requests, if requested by the data subject inform them of recipients.

RESPONSE CHECKLIST FOR DATA TRANSFER REQUESTS

Check that:

- The processing of the data is based on consent or contract.
- The processing of the data is carried out by automated means.

Check the response has included:

- Confirmation that the transfer has taken place.
- Confirmation that the transmitted data is in a structured, commonly used and machine-readable format.

Appendix C - Definitions

1. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future.
4. ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
5. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
6. ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
7. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

6. Information Security Incident & Personal Data Breach Procedure

PURPOSE

Bay Plastics. ('the Company', 'we', 'our', 'us') will ensure that it reacts appropriately to any actual or suspected security incidents and data breaches relating to information systems and information within its custody.

The purpose of this document is to describe the procedure for identifying, reporting and responding to information security incidents and managing a personal data breach.

An information security incident is an event that could breach our information security procedures. It may arise from:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- A deliberate attack on our systems.
- The unauthorised use of personal data by a member of staff.
- Misuse of information or equipment.
- Accidental loss or equipment failure.
- Changes to information or data or system hardware, firmware or software characteristics without the Company's knowledge, instruction or consent.
- The unauthorised use of a system for the processing or storage of data by any person.

This list is not exhaustive.

Nothing in this procedure shall prevent an employee from making a protected disclosure under the Employment Rights Act 1996.

SCOPE

This procedure applies to all those with authorised access to personal data processed by the Company irrespective of status, including employees, temporary staff, contractors, consultants and suppliers. Responsibilities of employees within this procedure also applies to all those within the scope.

ROLES & RESPONSIBILITIES

All employees have a responsibility to ensure the safe and secure use of information systems and information within the Company's custody and adhere to this procedure regardless of their status.

All employees have the responsibility to report any potential suspected or actual security incident immediately in order that any necessary action is taken to contain the incident, determine whether it constitutes a breach and meet the mandatory reporting requirements of the General Data Protection Regulations (i.e., to report within 72 hours of becoming aware of a breach).

Where an incident is accidental, the reporting procedure of the incident will be used to support employees learning and to improve processes.

However, incidents caused deliberately, by wilful neglect, non- compliance, including the non-reporting of an incident, may result in disciplinary action being taken in line with the Company's disciplinary policy and procedure.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

PERSONAL DATA BREACH

A personal data breach is defined as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Examples of information security incidents that could lead to a personal breach are in Appendix A.

Not all information security incidents are personal data breaches, but employees are required to report them for an assessment to be made by the Company.

REPORTING PROCEDURE - INFORMATION SECURITY INCIDENT / BREACH

Where an employee discovers or causes an information security incident/breach you must immediately:

1. **Contain** – If appropriate in the circumstances, take action to contain the incident, e.g., email recall, secure paper documentation.
2. **Report** – Advise the HR department. hr@bayplastics.co.uk If the HR department are not available you should advise the Managing Director or a senior manager. The employee will be asked to provide:

- What happened;
- When it happened;
- How it happened;
- How many people could be affected and the category of data subject(s);
- Any other detail relevant to the case.

3. **Maintain Confidentiality** – All employees have a duty to maintain confidentiality and contain the incident. Employees are not to:

- Discuss
- Share
- Store
- Copy

Information surrounding an information security incident / breach should not be shared with anyone other than those who are managing and / or investigating the incident. Doing so may compromise any containment, investigation or disciplinary proceedings in the future.

REPORTING PROCEDURE - VIRUS INFECTION

Security events, for example a virus infection, could quickly spread and cause data loss across the company. All employees must understand and be able to identify that any unexpected or unusual behaviour at work could potentially be a software malfunction. If an event is detected employees must:

- Note down (on paper, not the computer) the symptoms and any error messages ages on screen and;
- Advise the General Office Manager if an infection is suspected.

CONTAINMENT AND NOTIFICATION DECISIONS

The HR department will record the incident. All investigation and recovery actions, including date and time of action, name of person performing the action and if appropriate the name of the person approving the action will be recorded. The details recorded will be retained by the Company for the current year plus 6 years.

Any immediate measures will be implemented to limit damage already caused and to prevent further damage from occurring to the Company's reputation or assets or the organisation(s) we work with. The HR department and any other appropriate personnel will work with IT to do this.

For example, this could be isolating or closing a compromised section of the network, finding a lost piece of equipment, remotely wiping a device, securing storing files, changing access rights or codes and running audits activity reports.

The HR department and any other appropriate personnel will undertake an initial assessment to establish whether the incident constitutes a personal data breach. If concluded that it does, the Company has become "aware of the breach", so must:

- Where the Company are the "processor" and not the "Controller" of the personal data, report it to the appropriate "Controller" and comply with any contractual obligations imposed on the Company. The "Controller" is responsible for notification to relevant individuals.
- Where the Company are the "Controller" of the personal data, undertake a risk assessment to assess whether it meets the threshold to report to the Information Commissioners Office within 72 hours of becoming aware of the breach.
- Assess whether it meets the threshold to report to the affected individual(s).

The risk assessment will include taking into account:

- The type of breach – nature, sensitivity and volume of personal data.
- Ease of identification of individuals.
- Severity of consequences for individuals.
- Special characteristics of the individual.
- The number of affected individuals.
- Existing availability of the data.
- The existing technical and organisational measures that are in place to protect data.

The likelihood and security of risk will be determined for an overall decision of whether notification is to be made.

The Company will use the following guidance during the assessment – ICO Guidance and W29 Party Guidance.

Those involved in the containment and management of an incident could be:

- The Managing Director
- The HR department
- The Senior Leadership Team
- The IT team
- Project Managers
- External specialists

The Managing Director will make the final decision on notification with advice from the HR department and any other relevant parties.

Where a security incident occurs, which does not constitute a breach and the Company are acting as a "Processor" the Company will comply with any contractual obligations imposed on the Company to notify the "Controller".

NOTIFICATION

Where a decision is taken by the Company to notify, the Information Commissioners Office (ICO) within the 72 hours of becoming aware of the breach and provide:

- A description of the nature of the personal data breach including, where possible:

o The categories and approximate nature of the individuals concerned.

o The categories and approximate number of personal data records concerned.

o The name and contact details of the point of contact where more information can be obtained.

o A description of the likely consequences of the personal data breach and

o A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Where more information becomes known during further assessment and investigation, this needs to be brought to the attention of the ICO.

Where a decision is taken to notify the affected individual(s), it will be the HR department or any other appropriate personnel who will be appointed to contact them, without undue delay and provide the nature of the personal data breach and at least:

- The name and contact details of the nominated point of contact in the Company.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves. Therefore, depending on the nature of the breach and the risk posed, timely communication will help individuals take steps to protect themselves.

ONGOING ASSESSMENT OF RISK

In parallel with the containment and notification requirements, the HR department and any other appropriate personnel will be required to continue assessing risks associated with the incident to determine any further steps the Company should take.

It may be necessary to meet the individual who reported the incident to clarify how the incident occurred and seek confirmation that they have contained the incident. Where minutes of the discussion are taken these should be agreed by the individual.

It may be necessary to discuss with other key individual to make sure that details of the event remain fresh. Where minutes of the discussion are taken these should be agreed by the individual.

The IT team may be required to perform any necessary system audits, logs or checks to identify who has had access to the information and the type of activity. A decision will be taken on the need for identified individuals to be approached for a discussion to assist in assessing the risk.

Where appropriate a site visit will be undertaken, for example in cases involving theft, in order to familiarise the HR department and any other appropriate personnel with the incident which took place and make recommendations to avoid reoccurrence.

Recommendations may relate to, general security of premises, layout of the office, facilities for information storage.

Where the incident demonstrates deliberate action, wilful neglect and / or has a serious impact on the Company, the HR department and any other appropriate personnel, will determine the course of action. This may result in disciplinary action being taken in line with the Company disciplinary policy and procedure.

NOTIFICATION OF INCIDENT TO OTHER PARTIES

Consideration of other parties who should be notified is an important part of the incident management process.

The HR department and Managing Director will make a decision on notification content and the audience dependant on the nature of each individual case.

The list of parties to notify, in writing may include:

- The police, where theft or criminal activity is suspected.
- The media.
- Other third parties if the incident includes personal data provided by them.
- Other third parties/suppliers of their access has been restricted or denied.
- Third parties whereby they have interface / connection the Company's infrastructure, whereby a security incident may have an adverse impact on the connect or interface or the systems used at the opposing end.

EVALUATION & RESPONSE

The HR department and any other appropriate personnel with consider all circumstances around the incident, what policies and procedures are in place, what training has been received, was it a system or human error, was the incident caused by wilful neglect or accidental and has it happened before.

Dependant on the nature of the case, there may be a requirement to produce a full written record of the investigation and response which may include evidence to support any disciplinary or criminal prosecution actions that may be brought against an employee or other external entity. It may also include learning and whether there is a requirement to update current policies, procedures, processes and working practices, including this procedure.

The report will be kept by the HR department and provided to the Managing Director for consideration and distribution to the Senior Leadership Team. The HR department and any other appropriate personnel will evaluate the effectiveness of the response to the incident. The HR department will arrange for procedures to be updated, if necessary and communicated accordingly.

This is the current version of the Bay Plastics GDPR Policy, updated in September 2024 and it supersedes all previous versions.

If you have any questions or comments about this policy, please contact the Bay Plastics HR and Compliance department via one of the following channels:

HR & Compliance
Bay Plastics
Unit H1 High Flatworth
Tyne Tunnel Trading Estate
North Shields
Tyne & Wear
NE29 7UZ

+44 (0) 191 258 0777 - ask to speak to HR and Compliance Manager

hr@bayplastics.co.uk