Data/Privacy Policy (GDPR-compliant)

1. **INTRODUCTION**

1.1. This policy was last updated in March 2020.

1.2. As an organisation Kalsi Plastics (UK) Ltd collect, store and process personal data about our staff, customers, suppliers, supplier contacts, shareholders, website users and other third parties. This policy tells all staff how we comply with our legal obligations about people's personal data.

1.3. All employees, workers, contractors, agency workers, consultants, directors, members and others are expected to comply with this policy. It does not form part of any employee's contract of employment and may be amended at any time. Breach of this policy may result in disciplinary action.

1.4. All managers are responsible for ensuring compliance with this policy by their staff and are responsible for raising non-compliance with their managers in any case if they become aware of it. The person with overall responsibility for data compliance is Juggy Kalsi

2. **PERSONAL DATA PROTECTION PRINCIPLES**

3. We adhere to the principles relating to processing of personal data which require it to be:

3.1. Processed lawfully, fairly and transparently.

3.2. Collected only for specified, explicit and legitimate purposes.

3.3. Adequate, relevant and limited to what is necessary for the purposes for which it is processed.

3.4. Accurate and up to date.

3.5. Not kept in for longer than is necessary for the reason it is processed.

3.6. Processed securely to protect against unauthorised or unlawful processing and accidental loss.

3.7. Not transferred to another country without appropriate safeguards being in place.

3.8. Made available to data subjects on request, who can address issues of inaccuracy.

4. **LAWFULNESS, FAIRNESS, TRANSPARENCY**

4.1. We may only collect, process and share personal data fairly and lawfully and for pre-defined reasons. The permitted reasons are where:

4.1.1. The data subject has given their explicit consent;

4.1.2. The processing is necessary for the performance of a contract with them;

4.1.3. To meet our legal compliance obligations;

4.1.4. To protect their vital interests;

4.1.5. To pursue our legitimate interests for purposes (subject to the interests or fundamental rights and freedoms of the data subject).

4.2. These are the data we collect on employees and the grounds we rely on:

Data	**Purpose**	**Reason relied on**
Personal contact details such as name, address, telephone numbers, and personal email	So that we can contact you when you are not at work	To perform our contract with you and to send payroll documents such as payslips, P60's etc
Date of birth	So that we can calculate your entitlements and monitor diversity	To perform our contract with you; to meet our legal compliance obligations
Gender	So that we can monitor diversity	To meet our legal compliance obligations
Marital status and dependants	So that we can assess your entitlement to dependant's leave; to monitor diversity	To perform our contract with you; to meet our legal compliance obligations
Next of kin and emergency contact information	In case you have a medical emergency	To protect your vital interests
National Insurance number, copy of driving licence	To ensure compliance with tax and other laws	To meet our legal compliance obligations
Bank account details, payroll records and tax status information	To pay you accurately	To perform our contract with you; to meet our legal compliance obligations
Salary, annual leave, pension and benefits information	To pay you accurately	To perform our contract with you; to meet our legal compliance obligations
Start date and, if different, the date of your continuous employment	So that we can monitor diversity, calculate your entitlements and hold your s1 ERA statement of particulars	To perform our contract with you; to meet our legal compliance obligations
Leaving date and your reason for leaving	So that we can keep track of who we employ why they leave and when in case there is a dispute	To pursue our legitimate interests; to meet our legal compliance obligations
Recruitment information (including copies of right to work documentation, references and other information included in a CV)	So that we show that we employ qualified, skilled and experienced staff	To pursue our legitimate interests
Employment records (job titles, work history, working hours, holidays, training records and professional memberships)	So that we can pay you accurately	To perform our contract with you; to meet our legal compliance obligations
Performance, disciplinary and grievance information	So that we can show we employ staff who perform and behave to expectation and take fair disciplinary measures in cases of underperformance	To pursue our legitimate interests; to meet our legal compliance obligations
CCTV footage and other information obtained through electronic means such as swipe card	For reasons of security	To pursue our legitimate interests; to meet our legal compliance obligations

Information about your use of our information and communications systems	Our routine business communications will contain your details (eg in your signature) and for disciplinary reasons	To pursue our legitimate interests.
Results of HMRC employment status check, details of your interest in and connection with employment agencies through which your services are supplied	So that we show that we employ qualified, skilled and experienced staff	To meet our legal compliance obligations; to pursue our legitimate interests.

4.3. These are the special categories of data we collect on employees and the grounds we rely on:

Data	**Purpose**	**Reason relied on**
Details about your criminal convictions	So that we can comply with the Rehabilitation of Offenders Act and monitor risks to third parties, eg customers who may be exposed to risks by those who work for us	To meet our legal compliance obligations; to pursue our legitimate interests.
Your race or ethnicity, religious beliefs, sexual orientation and political opinions	So that we can monitor diversity and comply with our equality obligations	To meet our legal compliance obligations
Trade union membership	So that we can pay your subs and consult with the appropriate representatives about changes in the workplace	To meet our legal compliance obligations
Information about your health, including • Medical conditions, health and sickness records • Decisions relating to ill-health, injury or disability benefits; • Details of sickness absence from work • Where you leave employment and the reason for leaving is related to your health, information about that condition	So that we can make reasonable adjustments for disabilities, and record sickness absence accurately and pay you sickness benefits accurately	To meet our legal compliance obligations; to pursue our legitimate interests.

4.4. These are the data we collect on existing/prospective clients/customers and third parties and the grounds we rely on:

Data	Purpose	Reason relied on
Customer information including: • Company name, address, contact details, company registration and vat number, directors/employee details, trade references and bank details	So that we can setup customers on our system and invoice them correctly	To meet our legal and insurance obligations
Financial information accessed through credit check reports	So we can decide what credit facilities to offer credit customers	To meet our insurance obligations
Supplier information including: • Company name, address, contact details, company registration and vat number, directors/employee details, trade references and bank details	So that we can setup supplier on our system and pay them correctly	To meet our legal and insurance obligations

5. CONSENT

5.1. Consent must be explicitly given for us to use data for a particular purpose, which is why we set out the data and the reasons in the tables above. This is especially important where it comes to the special categories of personal data (very sensitive information).

5.2. Data subjects must be easily able to withdraw consent to data processing at any time. We will promptly honour requests to do this. If we don't have consent to use personal data for a different purpose for that for which we have consent, we will ask for consent for the new purpose.

5.3. Consent is not enough where it comes to our employees because of the imbalance of power between employee and employer. We should also rely on another of the reasons in para 4.1.

6. MONITORING OUR EMPLOYEES

6.1. The Company's systems enable us to monitor telephone, email, voicemail, internet and other communications.

6.2. In order to carry out our legal obligations as an employer (such as ensuring employees' compliance with our IT policies), and for other business reasons, we may monitor use of systems including the telephone and computer systems, and any personal use of them, by automated software or otherwise.

6.3. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

7. TRANSPARENCY

8. The GDPR requires us to provide detailed, specific information to data subjects and this policy complies with that at para 4 above.

9. Such information may also be provided through privacy notices (which must be concise, transparent, intelligible, easily accessible, and in clear and plain language) on an ad-hoc basis.

10. COLLECTED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

10.1. We will not use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purposes and (if necessary) they have consented.

11. ADEQUATE, RELEVANT AND LIMITED

11.1. Staff may only process personal data when their job duties require it. They must not collect excessive data. They must ensure any personal data collected is relevant to the intended purposes.

11.2. We must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines. These are that data is deleted after 6 years, unless a regulatory provision says otherwise.

12. ACCURACY

12.1. Personal Data must be accurate and kept up to date. It must be corrected or deleted without delay when inaccurate.

12.2. We must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

13. NOT KEPT IN FOR LONGER THAN IS NECESSARY FOR THE REASON IT IS PROCESSED

13.1. Personal data will not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. It can be anonymised for statistical purposes after that.

13.2. We will delete data after 6 years of it being needed, unless a regulatory provision says otherwise. Also we will require third parties to delete such data where they hold it on our behalf.

14. PROCESSED SECURELY

14.1. The measures we take to secure personal data are as follows;

14.1.1. Our HR data is kept in filing cabinets that are in a locked office and accessible only to those who need to use them.

14.1.2. Non-HR data in paper form is locked overnight and during the day it is not stored in places where unauthorised people can access it.

14.1.3. Electronic data is protected by the requirement to log onto a network with a username and password available only to authorised users.

14.1.4. Electronic data is stored in such a way that only those with the right access rights can access it.

14.1.5. We encrypt electronic data on our network and protect it against unauthorised access with a firewall and antivirus software.

14.1.6. We issue our staff with encrypted usb storage devices and require that they do not use unencrypted ones.

14.1.7. In common with most companies, our outgoing and incoming emails are not encrypted but we do not use email to send special categories of personal data. If we do need to send special categories of data via email (eg discussing employees' health with our lawyers), we will strip out identifying details such as names and relay that to the recipient by another means (eg telephone).

14.2. You will only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place.

14.3. We maintain data security by protecting the confidentiality, integrity and availability of personal data as follows:

Confidentiality means only people who need to know and are allowed to use personal data can access it.

Integrity means that personal data is accurate and suitable for the reason it is processed.

Availability means authorised users can access personal data when they need it for authorised purposes.

14.4. It is a disciplinary offence to attempt to circumvent the safeguards we have in place to protect personal data.

14.5. Breaching our IT policy may be a disciplinary offence depending on the circumstances.

15. REPORTING PERSONAL DATA BREACHES

15.1. We will notify any personal data breach to the Information Commissioner's Office and to the data subject where it creates a high risk to their rights and freedoms.

15.2. If a member of staff knows or suspects that a personal data breach has taken place, they should preserve all evidence relating to it and contact the person with overall responsibility for data compliance.

16. NOT TRANSFERRED TO ANOTHER COUNTRY WITHOUT APPROPRIATE SAFEGUARDS

16.1. We may transfer personal data within the EEA, where the GDPR applies.

16.2. Where data is transferred to other countries (eg using Dropbox, which is housed in the US, we will:

16.2.1. Ensure that the third party complies with data protection rights to an equal standard. For this purpose, we use the agreement in the Appendix.

16.2.2. Secure consent from the data subject after informing them of the risks or record the reason (that may be to perform a contract between us and the data subject, for reasons of public interest or in relation to pursuing or defending legal claims.

17. DATA SUBJECT RIGHTS AND REQUESTS

17.1. Data subjects have rights to:

17.1.1. See the data we hold on them;

17.1.2. Withdraw consent to data processing at any time;

17.1.3. Prevent us using their personal data for marketing;

17.1.4. See this policy;

17.1.5. Ask us to erase personal data if it is no longer necessary in for the reason for which it was collected or processed

17.1.6. Rectify inaccurate data or to complete incomplete data;

17.1.7. Challenge processing which we justify on the basis of legitimate interests or the public interest;

17.1.8. See a copy of an agreement under which personal data is transferred outside of the EEA;

17.1.9. Object to decisions based solely on automated processing, including profiling;

17.1.10. Be told of personal data breach likely to result in high risk to their rights and freedoms;

17.1.11. In some circumstances, to receive their personal data in a commonly used electronic format.

17.2. We will verify the identity of an individual requesting data under any of the rights listed above.

18. ACCOUNTABILITY – DEMONSTRATING COMPLIANCE

18.1. We have an obligation to put in place appropriate measures to ensure compliance with data protection principles. We must be able to demonstrate compliance with the data protection principles and this policy is our way of doing that.

18.2. We must train staff on data rights and maintain a record of training attendance by staff.

18.3. We must regularly test the privacy measures we have in place to assess compliance, including using results of testing to demonstrate compliance improvement effort.

19. RECORD KEEPING

19.1. The GDPR requires us to keep full and accurate records of all our data processing activities. This policy is part of how we do that.

20. DATA PROTECTION IMPACT ASSESSMENTS

20.1. We must conduct impact assessments in respect to high risk processing (where there is a high risk to the rights and freedoms of data subjects).

20.2. We will do this whenever we:

20.2.1. Implement a major system or business change involving the processing of personal data;

20.2.2. Use new technologies;

20.2.3. Start automated processing, profiling or automated decision-making; or

20.2.4. Process large scale quantities of special category data (eg health, sexuality or criminal convictions; and

20.3. An impact assessment will record:

20.3.1. A description of the processing

20.3.2. Its purposes

20.3.3. What our legitimate interests are for doing it

20.3.4. An assessment of the risk to data subjects

20.3.5. An assessment of the necessity and proportionality of the processing (an assessment of our needs weighed against those of the data subjects')

20.3.6. What measures are in place to minimise risk and show compliance

21. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

21.1. We do not conduct automated processing, profiling or automate decisions about individuals by using only a computer.

22. MARKETING

22.1. A data subject's prior consent is needed for unsolicited marketing (for example, by email). We can send unsolicited emails to email addresses that don't identify an individual (eg 'info@' but not otherwise

(eg ‘john.smith@’).

22.2. We are allowed to send unsolicited marketing to existing customers where “soft opt in” applies. This is where we have obtained contact details in the course of a sale to that person and gave them a clear opportunity to opt out of marketing every time we communicate to them.

22.3. If a customer opts out, their details will be removed from our marketing lists as soon as possible. We must retain just enough information to ensure that their preference is respected in future.

23. **SHARING PERSONAL DATA**

23.1. We are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. For sharing personal data with third parties, we use the agreement in the Appendix.

23.2. Staff may only share personal data we hold with another employee or representative of our company (including any sister companies and holding companies in the group) if the recipient has a job-related need to know and they comply with the rest of this policy.

24. We may share the personal data we hold with third parties, such as our service providers if:

24.1.1. They need to know the information for the purposes of providing the contracted services;

24.1.2. Sharing the personal data complies with this policy and any required consent has been obtained;

24.1.3. The third party agrees to comply with our data security standards and policy and has put adequate security measures in place;

24.1.4. Our contract with them includes suitable data protection clauses.

25. **CHANGES TO THIS PRIVACY STANDARD**

25.1. We reserve the right to change this policy at any time so please check back regularly to obtain the latest copy.

26. GLOSSARY

26.1. This is a list of terms that relate to data protection, some of which are used in this policy.

Automated Decision-Making (ADM)	When a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.
Automated Processing	Any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.
Consent	Agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject’s wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Controller	The person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.
Criminal Convictions Data	Personal data relating to criminal convictions and offences.
Data Subject	A living, identified or identifiable individual about whom we hold Personal Data.
Data Privacy Impact Assessment (DPIA)	An assessment tool used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data. We use the format in clause 20.
Data Protection Officer (DPO)	A person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance. We are not required to have a DPO.
EEA	The 28 countries in the EU, and Iceland, Liechtenstein and Norway.
Explicit Consent	Consent which requires a very clear and specific statement (that is, not just action). This policy uses the term 'consent' and we expect it to conform to this standard.
GDPR	The General Data Protection Regulation.
Personal Data	Any information identifying a Data Subject or information relating to them 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 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	Any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Privacy by Design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
Privacy Notice	Notices setting out information that may be provided to Data Subjects when we collect information about them. These notices may take the form of general privacy statements like this policy or a stand-alone, one time privacy statements for a specific purpose.
Processing	Any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. It includes transmitting Personal Data to third parties.

Pseudonymisation or Pseudonymised	Replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure. For example, if we were using employee data internally or sending it to a third party, we might replace individuals' details with a code and transmit that separately if required.
Special Categories of Personal Data	Information revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, health conditions, sexual life or sexual orientation.

APPENDIX: FORM FOR SHARING DATA WITH THIRD PARTIES

DEFINITIONS

Agreed Purposes	[List the purposes for which the personal data is to be held]
Permitted Recipients	The parties to this agreement, the employees of each party and any third parties engaged to perform obligations in connection with this agreement
Shared Personal Data	The personal data to be shared between the parties under clause 1.1 of this agreement. Shared Personal Data shall be confined to the following categories of information relevant to the following categories of data subject: [List the types of personal data to which this agreement relates]

1. **GENERAL**

1.1. This clause sets out the framework for sharing personal data between the parties. Each party acknowledges that one party (the Data Discloser) will regularly disclose to the other party (the Data Recipient) Shared Personal Data collected by the Data Discloser for the Agreed Purposes.

1.2. Each party shall comply with all the obligations imposed on a controller under data protection legislation and any significant breach of the that legislation by one party shall, if not remedied within 30 days of written notice from the other party, give grounds to the other party to terminate this agreement with immediate effect.

2. **OBLIGATIONS**

2.1. Each party shall:

2.1.1. Process the Shared Personal Data only for the Agreed Purposes;

2.1.2. Ensure that it has all necessary notices and consents in place to enable lawful transfer of the Shared Personal Data to the Permitted Recipients for the Agreed Purposes;

2.1.3. Give full information to any data subject whose personal data may be processed under this agreement of the nature such processing. This includes giving notice that, on the termination of this agreement, personal data relating to them may be retained by or, as the case may be, transferred to one or more of the Permitted Recipients, their successors and assignees;

2.1.4. Not disclose or allow access to the Shared Personal Data to anyone other than the Permitted Recipients;

2.1.5. Ensure that all Permitted Recipients are subject to written contractual obligations concerning the Shared Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this agreement;

2.1.6. Ensure that it has in place appropriate safeguards, reviewed and approved by the other party, against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

2.1.7. Not transfer any personal data received from the Data Discloser outside the EEA unless the transferor:

2.1.7.1. Complies with the provisions of Articles 26 of the GDPR (in the event the third party is a joint controller); and

2.1.7.2. Ensures that:

2.1.7.2.1. The transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 GDPR;

2.1.7.2.2. There are appropriate safeguards in place pursuant to Article 46 GDPR; or

2.1.7.2.3. One of the derogations for specific situations in Article 49 GDPR applies to the transfer.

2.2. Each party shall assist the other in complying with all applicable requirements of the data protection legislation. In particular, each party shall:

2.2.1. Consult with the other party about any notices given to data subjects in relation to the Shared Personal Data;

2.2.2. Promptly inform the other party about the receipt of any data subject access request;

2.2.3. Provide the other party with reasonable assistance in complying with data subject access requests;

2.2.4. Not disclose or release any Shared Personal Data in response to a data subject access request without first consulting the other party wherever possible;

2.2.5. Assist the other party, at the latter's cost, in responding to any request from a data subject and in ensuring compliance with its obligations under data protection legislation with respect to security, breach notifications, impact assessments and consultations regulators;

2.2.6. Notify the other party without delay on becoming aware of any breach of data protection legislation;

2.2.7. At the written direction of the Data Discloser, delete or return Shared Personal Data and copies of it when this agreement ends unless required by law to store it;

2.2.8. Use compatible technology for the processing of Shared Personal Data to ensure that there is no lack of accuracy resulting from personal data transfers; and

2.2.9. Maintain complete and accurate records and information to demonstrate its compliance with this clause 2.1 and allow for audits by the other party or the other party.

2.3. Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of data protection legislation by the indemnifying party, its employees or agents, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

27. **ACKNOWLEDGEMENT OF RECEIPT**

27.1. Our staff must all sign and return this policy to us with the following statement:

I acknowledge that I have received and read a copy of this privacy policy and understand that I am responsible for knowing and abiding by its terms.

Signed ……

Name ……

Dated ……