# DATA PROTECTION POLICY

# DATA PROTECTION POLICY

**CONTENTS PAGE**

## PART 1 - KEY UPDATES AND POINTS OF SIGNIFICANCE[1]

### 1. POLICY UPDATES

1.1 Effect of Brexit: The UK has left the European Union and the policy has been updated to make it clear that Section B applies to processing in both the UK and the EEA.

1.2 International transfers: The section on transferring / receiving data from the UK and the EEA has been updated to reflect recent case law (Schrems II). In particular, the EU-US Privacy Shield can no longer be used as a mechanism to legally transfer personal data to the US. If we rely on appropriate safeguards (such as the standard contractual clauses), we must also conduct a case by case assessment of the transfer to ensure it is subject to an adequate level of protection as required by the GDPR.

1.3 Following the end of the Brexit transition period, it might also be required to implement "appropriate safeguards" for transfers of personal data from the EEA to the UK if the UK does not receive an adequacy decision from the European Commission.

1.4 US requirements are set out in Section C of this policy.

### 2. PRACTICAL / PROCEDURAL IMPLICATIONS

2.1 Please review whether you or any service providers to your business have relied on the EU-US Privacy Shield to transfer personal data to the US and if yes, identify an "appropriate safeguard" to allow continued personal data flows to the US.

2.2 Please conduct a case by case assessment of all international personal data transfers from the UK and EEA to jurisdictions not considered adequate by the European Commission to determine if the transfers can continue and implement additional technical measures (where required).

2.3 Please consider whether appropriate measures are in place to be able to transfer personal data from the EEA to the UK (including Melrose Industries plc) at the end of the Brexit transition period on 31 December 2020.

2.4 Please consider whether your business is in scope of the CCPA and implement specific compliance programmes where required.

[1] Please note this is a non-exhaustive summary. The full policy should be reviewed and assessed for further training, practical and procedural implications and updates that are specific to your business.

## 3. TRAINING

3.1 The UK Information Commissioner's Office requires organisations to conduct regular data protection training in order to comply with the security and accountability principles under the GDPR. Induction and refresher data protection and information governance training should be provided to all staff and should incorporate national and sector-specific requirements. The security-related training requirements are provided by the ICO here. Senior management should sign off on the training programme.

3.2 If your business is subject to the CCPA, the CCPA also requires that "all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA to be informed of all requirements of the CCPA and the implementing regulations and how to direct consumers to exercise their rights under the CCPA and the implementing regulations."

## PART 2 – DATA PROTECTION POLICY

### A. BACKGROUND

1. **POLICY STATEMENT**

1.1 Individuals have rights with regard to how their personal data is handled. During the course of our activities we will collect, store and process personal data about our staff, customers, suppliers and other third parties. We recognise the need to treat this information in an appropriate and lawful manner, depending on the laws that apply to the processing of it.

1.2 This data protection policy is designed to assist in ensuring we do so and that we manage the data protection risks arising out of our activities. Application of this policy allows us to align procedures with the legal obligations to which we are subject and to good practice.

1.3 This policy applies to Melrose Industries plc and its businesses ("we, "us", "our"). This policy has been approved by the board of directors of Melrose Industries PLC, who are responsible for ensuring this policy complies with relevant legal and ethical obligations.

The General Counsel for each business within the Group is responsible for ensuring awareness of and compliance with this policy within their particular business unit.

Each business within the Group is expected to establish a "culture" of compliance with this policy. The executive team of each business must take direct responsibility for ensuring effective transmission of this policy throughout their business unit, together with relevant guidance and training, and appropriate safeguards, monitoring, and resources, in order to ensure compliance with this policy.Melrose Group business units may have a specific Data Protection Policy applicable to them which they will need to follow.

1.4 In Europe, the Melrose Group is exposed to potential fines of up to €20 million (currently approximately £18 million or $24 million) or 4% of total worldwide annual turnover, whichever is higher, for failure to comply with the provisions of the European Union General Data Protection Regulation ("GDPR"). In the United States, the Melrose Group is exposed to fines and enforcement actions from the various regulators that have authority over it, as well as class action and other lawsuits.

1.5 This policy has been approved by the board of directors of Melrose Industries PLC. All employees, contracts, agency staff and other

personnel[2] must comply with this policy. Any breach of this policy will be taken seriously and may result in disciplinary action.

## 2. ABOUT THIS POLICY

2.1 The types of information that we may handle include details of current, past and prospective employees. It can also include information about suppliers, customers and others that we communicate with (and/or, when they are companies, the individuals within them with whom we deal).

2.2 This information, which may be held on paper, on a computer or other media, or in the cloud, is subject to certain legal safeguards. Legal obligations to which we are subject impose restrictions on how we may use that information.

2.3 Where personal data has been collected or processed in the United Kingdom ("UK") or the EEA by us or third parties, or where personal data about data subjects in the UK or the EEA has been collected or processed by us or third parties from outside the UK and the EEA in the course of delivering goods or services to such data subjects, or monitoring their behaviour (for example, with CCTV), in the UK or the EEA, we must comply with applicable data protection laws (such as the UK Data Protection Act 2018 and the GDPR) when we process it (including where we transfer that personal data to other companies in the Melrose Group or third parties). Part B of this policy applies to such processing.

2.4 Where personal data has been collected or processed by us in the United States or relates to data subjects located in the United States, we must comply with the laws that apply to the use of personal data in the United States. Part C of this policy applies to such processing.

2.5 Where personal data has been collected or processed outside United Kingdom, EEA and the United States, we must comply with the laws that apply to the use of personal data in those countries.

2.6 The policy may be amended at any time by the issuing of a replacement policy.

## 3. ENSURING COMPLIANCE WITH THIS POLICY

3.1 The Head Office legal team is responsible for ensuring compliance with this policy and is contactable by email at Warren.Fernandez@melroseplc.net.

3.2 Any questions or concerns about the operation of this policy should be referred in the first instance to the legal team. If you consider that

[2] For convenience, this Policy uses the terms "employee" and "staff" to include all such people.

the policy has not been followed in respect of personal data (whether about yourself or others) you should raise the matter with the legal team.

## 4. DEFINITION OF DATA PROTECTION TERMS

4.1 In this policy, we use the following terminology:

**Criminal convictions data** means personal data relating to criminal convictions and offences.

**Data** is information which is stored electronically, on a computer, or in highly organised paper-based filing systems.

**Data privacy impact assessment (or DPIAs)** means the tools and assessments used to identify and reduce risks of a data processing activity. A data privacy impact assessment should be conducted for all major system or business change programs involving the processing of personal data.

**Data subjects** include all living individuals ("natural persons") about whom we hold personal data. A data subject need not be a national or resident of a country in which we are incorporated or operate. All data subjects (irrespective of nationality or residency) have legal rights in relation to their personal data.

**Data controllers** are the organisations which determine the purposes for which, and the manner in which, any personal data is processed. In many jurisdictions, they have the responsibility to establish practices and policies in line with data protection law. Each Melrose Group company is the data controller of all personal data used in and as part of its business.

**Data processors** include any company or other person which processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition. It will include suppliers which handle personal data on our behalf.

**Data users** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

**EEA** means the member states of the European Union and Iceland, Liechtenstein and Norway.

**Personal data** means data relating to a living individual ("natural persons") who can be identified from that data (or from that data and other information in our possession or which we can reasonably access). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal or statement as to credit-worthiness). Personal data includes sensitive personal data (see definition below). Note that the definition of

personal data under the GDPR and that of personal information under state law in the United States may also vary.

**Personal data breach** means any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The actual or reasonably suspected loss, misuse, or compromise, or unauthorised access, destruction, alteration, disclosure or acquisition, of personal data is also a personal data breach.

**Privacy** by design and by default is an approach to take when performing a project, implementing technology or using data in a new or different way that will involve the use of personal data that ensures that, as a matter of standard practice, a person's rights in their personal data (and our obligations with respect to it as detailed in the policy) and any adverse effects there may be to this by the adoption of the project, technology or use of data are identified and considered from the outset of that particular project, implementation action or use of data and are taken into account as part of the design and implementation phases to ensure that any adverse effects are minimised to the extent possible to ensure compliance with the GDPR. Projects where a privacy by design approach should be taken may include, for example:

- building new IT systems for storing or accessing personal data;
- embarking on a data sharing initiative; or
- using data for new purposes.

**Processing** is any activity that involves use of the data. It includes collecting, obtaining, recording, storing or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

**Pseudonymisation** means 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.

**Sensitive personal data** means special categories of personal data and criminal convictions personal data. Other categories of sensitive personal data may apply depending on the jurisdiction. In the United States, sensitive personal data categories include, but are not limited to: age, disability, national origin, race, colour, religion, sex, genetic and biometric information, sexual orientation, medical condition,

military or veteran status, financial information, social security numbers, health information, and account username and password.

Sensitive personal data can only be processed under strict conditions, and will often require the express consent of the person concerned. A data privacy impact assessment may need to be carried out before sensitive personal data can be processed. Please contact the legal team for further information and for assistance completing a privacy impact assessment.

**Special categories of personal data** means personal data revealing or concerning a person's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- physical or mental health conditions;
- sexual life or sexual orientation; and
- genetic data, or biometric data for the purpose of uniquely identifying such person.

## B. EUROPEAN REQUIREMENTS: HANDLING PERSONAL DATA THAT HAS BEEN PROCESSED IN THE UK OR THE EEA

### 5. THE FUNDAMENTAL EUROPEAN DATA PROTECTION PRINCIPLES

5.1 This Part B applies where we process personal data in the UK or the EEA or where we have received personal data from a party (such as another member of the Melrose Group or a third party) in the UK or the EEA under a data transfer agreement (see section 16 below) or we have received personal data from an individual residing in the UK or the EEA where we are offering them goods or services or monitoring their behaviour (e.g. tracking or profiling online browsing of our websites) in some way. Where that is the case, we must comply with the following principles of good practice. We must ensure that personal data is:

5.1.1 Processed lawfully fairly and in a transparent manner;

5.1.2 Processed for specified, explicit and legitimate purposes;

5.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes;

5.1.4 Accurate and where necessary kept up to date;

5.1.5 Not kept longer than necessary for the purpose;

5.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, damage or destruction;

5.1.7 Not transferred to people or organisations situated in countries without adequate protection; and

5.1.8 Made available to data subjects on request and data subjects are allowed to exercise certain rights in relation to their personal data.

5.2 The remainder of this policy describes our requirements in relation to these principles.

### 6. FAIR AND LAWFUL PROCESSING

6.1 This policy (like much European data protection law) does not prohibit the processing of personal data, but rather it seeks to ensure that it is done fairly, without adversely affecting the rights of the data subject.

6.2 We need to ensure that data subjects know that data is being processed by us and for what specified lawful purpose. Almost always this will be obvious from context and that will often suffice

(depending on local law) without anything formal being done. However, a specific "data protection notice" should be considered whenever paper or website forms are created which collect details and seek to obtain permission for processes involving the processing of personal data (such as recruitment purposes or direct marketing activities).

6.3 For personal data to be processed fairly and lawfully, it must only be processed for a lawful purpose specified by European data protection law. The four specified lawful purposes which are likely to be relevant to our activities are that:

6.3.1 the data subject has consented to the processing;

6.3.2 the processing is necessary for us to comply with a legal obligation;

6.3.3 the processing is necessary to enter into or perform a contract with the data subject; or

6.3.4 the processing is necessary for the purpose of our legitimate interest or a legitimate interest of a party to whom the data is disclosed where that interest is not overridden because the disclosure prejudices the interests or fundamental rights and freedoms of the data subject(s). The purposes for which we process personal data for legitimate interests need to be notified to the data subject(s) (for example, in an applicable privacy notice).

6.4 When sensitive personal data is being processed, more than one condition must be met. When the sensitive personal data is that of an employee, it can be processed if it is necessary for the data controller to discharge an obligation imposed upon it by employment law. In most other cases the data subject's explicit consent to the processing of such data will be required. A privacy impact assessment may need to be carried out before sensitive personal data can be processed. Please contact the Melrose Legal Ream for further information and for assistance completing a privacy impact assessment.

6.5 You must identify and document the legal ground being relied on for each processing activity.

## 7. PROCESSING FOR LIMITED PURPOSES

7.1 Personal data must only be processed for the specific purposes identified when the data was first collected or for any other purposes specifically permitted by applicable law. This means that personal data should not be collected for one purpose and then used for another. For example, data about staff collected for HR

purposes should not be used (post-employment) for the purposes of direct marketing. If it becomes necessary to change the purpose for which the data is processed, where applicable law requires this, the data subject must be informed of the new purpose before any processing occurs.

**Employee and pension scheme member Data**

7.2 Data about staff (including past and prospective staff) may be processed for legal, personnel, administrative and management purposes in the data controller's (the employing entity's) legitimate interests and to enable the data controller to meet its legal obligations as an employer or to perform a contract with them, for example to pay staff, monitor their performance and to confer benefits in connection with their employment. Data about members of the pension scheme may be processed for the purposes of administering the scheme or conferring benefits under the scheme, which will be in the employing entity's or pension scheme's legitimate interests.

**Customer Data**

7.3 We process data about our customers (including potential customers). Any personal data we hold will generally be about individual representatives of our customers and typically will include contact and other biographical details. We may process this personal data for administrative and account management purposes such as servicing the needs of our customers. It would be unusual for us to process any sensitive personal data about our customers or their representatives.

**Supplier Data**

7.4 We also process data about our suppliers (including potential suppliers). Any personal data we hold will generally be about individual representatives of our suppliers and typically will include contact and other biographical details. We may process this personal data for administrative and account management purposes. Again, it would be unusual for us to process any sensitive personal data about our suppliers or their representatives.

## 8. TRANSPARENCY

8.1 European data protection law requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. This information must be provided through appropriate privacy notices or fair processing notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject may easily understand them.

8.2 Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subjects with all the information required by European data protection law, which under the GDPR includes the identity of the data controller, how and why we will use, process, disclose, protect and retain that personal data through a privacy notice which must be presented when the data subject first provides the personal data.

8.3 When personal data is collected indirectly (for example, from a third party or publically available source), you must provide the data subject with all the information required by the GDPR as soon as possible after collecting or receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplated our proposed processing of that personal data.

## 9. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

9.1 Personal data must be adequate, relevant and limited to what is necessary for the specific purpose identified at the time of collection. Any data which is not necessary for that purpose should not be collected in the first place.

9.2 You must ensure that when personal data is no longer needed for its specified purposes, it is deleted or anonymized in accordance with the applicable document retention policy.

## 10. ACCURATE DATA

10.1 We must ensure that personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date personal data should be amended or destroyed.

10.2 Employees who become aware of any information that is inaccurate should inform their line manager or the local human resources team as appropriate.

## 11. DATA RETENTION

11.1 Personal data must not be kept for longer than is necessary for the specified lawful purpose for which it is processed. This means that data should be destroyed or erased from our systems when it is no longer required, in accordance with the applicable document retention policy. This includes requiring third parties to delete such personal data where applicable.

11.2 The document retention policy has been created to ensure that personal data is deleted after a reasonable time for the purposes for which it was being held.

11.3 You will ensure data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

11.4 Any member of staff who receives a written request should forward it to their line manager or local human resources team immediately.

## 12. DATA SUBJECTS' RIGHTS AND REQUESTS

12.1 Data should be processed in line with data subjects' rights. Their rights include the following:

12.1.1 the right to request access to any personal data held about them by a data controller;

12.1.2 the right to prevent the processing of their personal data for direct-marketing purposes;

12.1.3 the right to ask to have inaccurate personal data amended;

12.1.4 withdraw their consent to processing at any time;

12.1.5 receive certain information about the data controller's processing activities;

12.1.6 ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate personal data or to complete incomplete personal data;

12.1.7 restrict processing in specific circumstances;

12.1.8 challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

12.1.9 request a copy of an agreement under which personal data is transferred outside of the UK or the EEA;

12.1.10 object to decisions based solely on automated processing, including profiling;

12.1.11 prevent processing that is likely to cause damage or distress to the data subject or anyone else;

12.1.12 be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;

12.1.13 in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

12.1.14 You must verify the identity of an individual requesting personal data under any of the rights listed above (do not allow third parties to persuade you into disclosing personal data without proper authorisation).

## 13. DATA SECURITY

13.1 We should always ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

13.2 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

13.2.1 Confidentiality means that only data users who are authorised to use the data can access it.

13.2.2 Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

13.2.3 Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

13.3 We are required to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction that are appropriate to our size, scope and business over available resources, the amount of personal data that we own or maintain on behalf of others and identified risks. The procedures that we implement and maintain should include (but are not limited to):

13.3.1 Entry controls. Any stranger seen in entry-controlled areas should be reported.

13.3.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal data is always considered confidential).

13.3.3 Methods of disposal. Paper documents should be shredded. Memory sticks, CD-ROMs, etc. should be securely wiped and physically destroyed when they are no longer required.

13.3.4 Equipment. Data users should ensure that individual monitors do not show confidential information to

passers-by and that they use a security shield, password protected screen saver or log off from their PC when it is left unattended.

13.3.5 Staff records should be available only to members of the human resources department or appropriate senior management. It is important that offices and cabinets within the human resources department are locked when unattended. All electronically stored staff data should be on dedicated drive/devices, to which only HR staff (and responsible IT staff for maintenance purposes) have access.

13.3.6 Customer data should be stored in a central Customer Relationship Management ("CRM") system only. Only employees with a business need to access the data should be permitted to.

13.3.7 Data users must not store personal data on their own PC drives or other devices. Data should instead be stored on centrally provided servers so as to benefit both from encryption and from our back-up regime.

13.3.8 CCTV. Images should be:

- protected including during transmission (e.g. if by wireless means);
- subject to restrictions so that only appropriate (and trained) staff can access them;
- stored in controlled and secured rooms and systems; and
- processed only in accordance with section 18 below.

## 14. CUSTOMER RELATIONSHIP MANAGEMENT SYSTEMS

14.1 It is important to remember when using any CRM tool that data subjects (including employees and customer and supplier representatives) have rights under data protection laws, including the right to access their personal data and the right to object to direct marketing.

14.2 Data users should ensure that they do not enter into the CRM system any negative opinion or any other information which might reflect badly on the Melrose Group if the relevant data subject were to become aware of it. If there is an issue about an individual which others in the Melrose Group should be aware of that should be

recorded with a statement to contact you: such as "Contact [YOUR NAME] before contacting this person".

14.3 Care should be taken in relation to entering any sensitive personal data into a CRM system. The considerations set out at section 6.4 above will apply. It is likely that express consent of the data subjects would be needed in many situations.

14.4 Rules around the sending of marketing materials will depend on local law. In some countries, for example, marketing materials may not be sent by email unless the recipient has "opted-in". These rules should be respected.

14.5 In any case, opt-outs from marketing should always be respected. If any individual indicates that they do not want to receive marketing materials that should be recorded on the CRM database used. You should also make others who might send such information aware.

## 15. PROVIDING INFORMATION TO DATA PROCESSORS

15.1 On occasions, we will need to engage the assistance of third party service providers who will have access to personal data to provide their services. Examples of this are when we appoint outsourced technology providers, payroll services or health insurance providers or auditors.

15.2 Before we transfer any personal data to any data provider:

15.2.1 We should consider if the data processor has a need to know the information for the purposes of providing the contracted services;

15.2.2 We are satisfied that sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;

15.2.3 We should undertake appropriate checks to make sure such a processor adheres to at least equivalent procedures and policies to those applied throughout the Melrose Group and provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner to meet the requirements of the GDPR and, if applicable, ensure the provision of the rights of the data subject;

15.2.4 We should ensure the data processor enters into a written contract which contains a contractual commitment from the service provider to this affect and which complies with the requirements for such contracts under the GDPR (you should discuss these requirements

with the legal team if you are unsure about what is necessary in order to comply with the GDPR);

15.2.5 We should ensure the transfer complies with any applicable cross-border restrictions for transfers of personal data; and

15.3 We should undertake ongoing monitoring to ensure that data processors comply with these commitments (the extent of the monitoring will be dependent on the nature of the service provision).

## 16. TRANSFERRING / RECEIVING PERSONAL DATA FROM THE UK AND THE EUROPEAN ECONOMIC AREA: ENSURING ADEQUATE PROTECTION

16.1 Organisations that collect and otherwise process personal data in the UK or the EEA are required to do so in compliance with European data protection laws that prohibit the transfer of personal data to parties that are located outside the UK or the EEA unless adequate protections exist. Personal data is transferred if it is transmitted, sent, viewed or assessed to a different country.

16.2 To the extent that one of our companies located in the UK or the EEA wishes to transfer or grant access to the personal data to other parties (such as other members of the Melrose Group or third parties) that are located outside the UK or the EEA, that company can only do so if one of the following condition applies:

16.2.1 the recipient is located in a jurisdiction which the European Commission has decided offers adequate protection (as of September 2020, these jurisdictions are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay);

16.2.2 the personal data transfer is subject to 'appropriate safeguards' listed in the GDPR such as that the recipient:

(a) Agrees to enter into a standard form data transfer agreement approved by the European Commission for this purpose called the standard contractual clauses; or

(b) Is subject to an approved code of conduct or certification together with binding and enforceable commitments of the recipient in the third country to apply the appropriate safeguards, including as regards data subjects' rights;

and we have determined that such personal data transfer is subject to an adequate level of protection as required by the GDPR, taking

into account the circumstances of the transfer (including the local law in the jurisdiction of the recipient) and any supplementary measures implemented;

16.2.3 the data subject has provided their explicit consent to the proposed transfer after being informed of any potential risks; or

16.2.4 the transfer is necessary for one of the other reasons set out in the UK Data Protection Act 2018 or the GDPR.

16.3 Our companies in the UK or the EEA must not transfer personal data to an entity which is located in a country outside the UK or the EEA (including to a member of the Melrose Group outside the UK or the EEA) unless we are satisfied that appropriate contractual or other arrangements are in place to protect the personal data as explained in section 16.2 above.

16.4 Following the end of the Brexit transition period, it might become necessary that for transfers of personal data from one of our companies or third parties in the EEA to one of our companies or third parties in the UK, we will need to implement one of the 'appropriate safeguards' for such transfers referred to in section 16.2.2 above. You should discuss these requirements with the legal team if you are unsure about what is necessary in order to comply with the GDPR.

## 17. PROVIDING PERSONAL DATA TO OTHER THIRD PARTIES

17.1 There will be occasions when we are asked or obliged to provide personal data to third parties (who are not data processors); for example, to government agencies, tax authorities, law enforcement agencies or when required by a court order. We may also be asked to provide personal data as part of a reference for a former employee.

17.2 Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal data. In particular they should:

17.2.1 Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested.

17.2.2 Ask the third party to put their request in writing so that the third party's identity and entitlement to the information may be verified.

17.2.3 Ensure that there is a specified lawful basis for disclosing the personal data before agreeing to make the disclosure.

17.2.4 Refer to the legal team for assistance in difficult situations.

17.2.5 Where providing information to a third party, do so in accordance with the data protection principles set out in section 5 above (for example, sending only that personal data which is necessary for the specified lawful purpose), including, if legally required or otherwise whenever possible, putting a written agreement in place with the third party that will detail how they will use the personal data provided to them. If the personal data will be transferred outside of the UK or the EEA the requirement set out in section 16, with respect to cross-border transfers must be met.

## 18. CLOSED CIRCUIT TELEVISION

18.1 When we install Closed Circuit Television ("CCTV") on our premises, we should be clear about the reasons for installation: for example, whether it is as a security measure or alternatively as a measure for monitoring employees. A privacy impact assessment may need to be completed to ensure that we comply with our data protection obligations. Please speak to the legal team for further details about how to complete this.

18.2 We will not install such surveillance in areas where there is a heightened expectation of privacy (such as in changing rooms or toilet areas) except in the most exceptional circumstances where it is necessary to deal with very serious concerns.

18.3 We will display clear and prominent signs to let people know that CCTV surveillance is being carried out. Signs will be placed at the entrance of the CCTV zone and inside the surveilled area.

18.4 Surveillance cameras will not be used to record conversations between members of the public as this is regarded as highly intrusive and unlikely to be justified under applicable law.

18.5 When we receive a request (for example, from law enforcement agencies) in relation to disclosure of any images made, section 17 above will apply.

18.6 We will comply with local legal requirements in relation to the retention of images. In any case, images should be destroyed after 30 days unless an incident is reported that requires further investigation.

## 19. ACCOUNTABILITY

19.1 We must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to

demonstrate, compliance with the data protection principles. We must have adequate resources and controls in place to ensure and to document GDPR compliance including:

19.1.1 implementing privacy by design when processing personal data and completing DPIAs where processing might present a high risk to rights and freedoms of data subjects;

19.1.2 integrating data protection into internal documents including in compliance with this policy, related policies or privacy notices/fair-processing notices;

19.1.3 training our personnel on data protection compliance in accordance with section 21.1 below; and

19.1.4 testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance in accordance with section 21.2 below, including using results of testing to demonstrate compliance improvement effort.

## 20. RECORD KEEPING

20.1 The GDPR requires us to keep full and accurate records of all our data processing activities.

20.2 We must keep and maintain accurate corporate records reflecting our processing including records of consents given by data subjects and procedures for obtaining consents.

20.3 These records should include, at a minimum, the name and contact details of the data controller, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the details set out above together with appropriate data flows.

## 21. TRAINING AND AUDIT

21.1 We are required to ensure all personnel have undergone adequate and regular training to enable them to comply with data privacy laws. The training should be comprehensive and cover the GDPR, this policy, related policies and data protection matters including, for example, data subjects' rights, consent, legal basis for processing, DPIAs and personal data breaches. The training should also incorporate sector-specific requirements and any applicable local laws. The senior management of the Melrose Group should

sign off on this training. We must maintain a record of training attendance by our personnel.

21.2 We must also test our systems and processes to assess compliance and that they meet appropriate technical and organisational measures. We will periodically review the systems and processes under our control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

## 22. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

22.1 We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. We must assess what privacy by design measures can be implemented on programs/systems/processes that process personal data by taking into account the following:

22.1.1 the technology available;

22.1.2 the cost of implementation;

22.1.3 the nature, scope, context and purposes of processing; and

22.1.4 the risks to the individuals concerned by the processing.

22.2 We must also conduct a data protection impact assessment ("DPIA") if any processing of personal data is likely to have high risks to the privacy or other rights of the individuals concerned. If you believe this is likely to be the case, please contact the legal team who can help you complete a DPIA.

## 23. AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

23.1 Broadly, profiling means gathering information about an individual (or group of individuals) and analysing their characteristics or behaviour patterns in order to place them into a certain category or group, and/or to make predictions or assessments about, for example, their:

23.1.1 ability to perform a task;

23.1.2 interests; or

23.1.3 likely behaviour.

23.2 Under the GDPR, automated decision-making is the ability to make decisions by technological means without human involvement.

Automated decisions can be based on any type of personal data, for example:

23.2.1 personal data provided directly by the individuals concerned (such as responses to a questionnaire);

23.2.2 personal data observed about the individuals (such as location data collected via an application);

23.2.3 derived or inferred personal data such as a profile of the individual that has already been created.

23.3 Generally, automated decision making and profiling is prohibited when a decision has a legal or similar significant effect on an individual unless:

23.3.1 the data subject concerned has explicitly consented;

23.3.2 the processing is authorised by law; or

23.3.3 the processing is necessary for the performance of or entering into a contract.

23.4 A "legal effect" is a processing activity that has an impact on someone's legal rights, whether that be statutory or contractual.

23.5 A decision that has a "similar significant effect" is a decision that may lead to the exclusion or discrimination of individuals. The GDPR gives the example of "automatic refusal of an online credit application" or "e-recruiting practices without any human intervention".

23.6 We do not undertake any profiling or automated decision making using personal data.

## 24. DIRECT MARKETING

24.1 We are subject to certain rules and privacy laws when marketing to our customers.

24.2 For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

24.3 The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

24.4 A data subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

## C. US REQUIREMENTS

### 25. FEDERAL LAW

25.1 U.S. Federal law does not impose a comprehensive data security or data privacy regulatory framework. Rather, it applies a sectoral approach, giving different federal agencies regulatory and enforcement authority over different sectors of the economy.

25.2 To the extent our data collection or engagement with employees, customers, vendors, or suppliers in the United States subjects it to the authority of specific regulators such as the Federal Trade Commission, the Consumer Financial Protection Bureau, and the Securities and Exchange Commission, among others, it will comply with all attendant legal obligations.

25.3 The Federal Trade Commission has authority to enforce against data privacy and security violations. Personal data collected from data subjects in the U.S. must be processed in accordance with any applicable privacy notices and other disclosures made to data subjects concerning the processing of their personal data. To the extent any personal data must be shared or transferred to a third party, we must ensure that sharing or transferring the personal data complies with any privacy notice provided to the data subject. Violating a promise made in a privacy notice may subject us to an enforcement action for unfair or deceptive acts or practices brought by the Federal Trade Commission or state attorneys general.

25.4 To the extent we are engaging in marketing emails with customers in the United States, we must comply with the CAN-SPAM Act. The law makes no exception for business-to-business emails. We must ensure marketing emails comply with the requirements of CAN-SPAM and customers have the right to opt-out from marketing emails. Opt-outs from marketing should always be respected. If any individual indicates that they do not want to receive marketing materials that should be recorded on the CRM database used. You should also make others who might send such information aware.

25.5 With respect to employee personal data:

25.5.1 To the extent we seek a background information report for employment purposes, the company must comply with the Fair Credit Reporting Act ("FCRA"). This means that we must first disclose in writing to the employee or applicant that a background information report is being obtained and the employee or applicant must authorize in writing that the report may be obtained. In addition, if the report may result in an adverse employment action, we must provide the employee or applicant with a pre-adverse employment action notice, a copy of the report, and a description of the employee's rights under the FCRA. The person then will have an opportunity to review the report and explain any negative information prior to us taking any adverse action.

25.5.2 U.S. federal laws, such as the Wiretap Act and the Electronic Communications Privacy Act, and state laws regulate live or "real-time" workplace surveillance activities, such as video surveillance, recording of telephone calls, and interception of electronic communications. Accessing stored communications (such as an email or text message in storage) is governed by the Stored Communications Act under U.S. Federal law and applicable state laws.

(a) With respect to CCTV or other video surveillance used in the workplace, we can use CCTV or other video surveillance as long as such recordings do not have audio recording and are not in a private area, such as a restroom, locker room, or private office. Some states also require that we provide notice of the surveillance and that cameras are not hidden.

(b) With respect to recording telephone calls and other communications, state laws vary between requiring the consent of one party to requiring the consent of all parties to the conversation. It is best practice to comply with the all-party consent requirement for all states. Therefore, in general, we may record telephone calls in the following situations: (i) all parties to a communication consent to the recording, (ii) the device used to record the communication (e.g., telephone) is provided by us and the recording is done in the ordinary course of business, (iii) the employee has been provided prior notice that communications on Melrose Group devices may be recorded, and (iv) we are providing the

communications service and are acting in a way necessary to render the service or protect the rights or property of the service. Each state may also have different employment laws that apply to the recording of employees, so please discuss with the legal team before proceeding with any such recording.

(c) With respect to accessing communications stored on Melrose Group-provided electronic equipment, we may access these in a manner consistent with the our acceptable use policies that were disclosed to the employees. We must obtain permission from an employee prior to accessing communications that are stored elsewhere, such as an employee's private social media account or personal email account.

25.6 We may receive requests from the U.S. government, law enforcement, or other third party as part of an investigation to produce certain information, including personal data. Determining what information may and may not be produced under U.S. law can be complex. Sometimes statutes require the production of information, such as when a court issues a subpoena, but prohibit the production of information when a subpoena does not exist. Any employee who receives such a request must refer the request to the legal team for assistance.

25.7 If we identify business activities or data collection activities in the United States that are subject to specific regulatory oversight, then we will review regulations and relevant enforcement actions to clarify our legal obligations.

## 26. STATE LAWS

26.1 To the extent we process personal data from California residents, the California Consumer Privacy Act ("CCPA") and the California Attorney General's implementing regulations ("CCPA Regulations") may apply.

26.1.1 Employee Data. Personal data collected from California residents by us in the employment context (i.e., from our employees) is exempted from the majority of the CCPA's obligations until 1 January 2022. However, this exemption does not apply to our obligation to inform such employees, at or before the point of collection, of the categories of personal data collected from such data subjects and the purposes for which the personal data will be used.

26.1.2 Consumer Data. We currently do not collect personal data from consumers. However, if it does in the future, then we will need to comply with the CCPA's obligations with respect to the personal data of any consumers who are California residents. Such obligations include providing a notice at collection, providing a privacy policy, and providing the consumers with certain rights to their personal data.

26.2 Most states (e.g., California, Colorado, Massachusetts, New York) have enacted cybersecurity statutes and regulations. To the extent we process certain sensitive personal data of data subject residing in such states, these cybersecurity statutes and regulations will apply. Some of these laws also have specific contractual requirements for service providers that will be processing personal data on our behalf. For example, if we are processing certain sensitive personal data of Massachusetts resident, we are required to implement a comprehensive information security program, which includes, secure storage, encryption of all data transmitted and stored on portable devices, user authentication protocols, access restrictions to personal data, monitoring of third-party vendors, and workforce security training. In addition, depending on the types of sensitive personal data that the we are processing, additional privacy and security requirements must be met in order to appropriately safeguard the processing of such personal data.

26.3 All 50 U.S. states, as well as certain U.S. districts and territories such as Washington DC and Puerto Rico, have established data breach notification laws that apply in the event of an actual or reasonably suspected personal data breach. These data breach notification laws vary and impose their own distinct obligations on U.S. entities. Therefore, where we have an actual or reasonably suspected personal data breach that affects the data of residents from those jurisdictions, we should review the applicable state data breach notification laws to clarify our legal obligations.

26.4 As a general matter, many of these laws require notification to affected individuals, credit reporting agencies, state officials, and/or law enforcement in the event of a data breach of a delineated size.

26.5 If you identify a data breach involving U.S. information, please contact Warren Fernandez (Warren.Fernandez@melroseplc.net), Garry Barnes (garry.barnes@melroseplc.net) and Jason Care (Jason.Care@melroseplc.net) immediately to determine any necessary compliance obligations.

## D. GENERAL REQUIREMENTS

### 27. SECURITY BREACHES RELATING TO PERSONAL DATA

27.1 If you suspect that a personal data breach has occurred, please contact Warren Fernandez (Warren.Fernandez@melroseplc.net), Garry Barnes (garry.barnes@melroseplc.net) and Jason Care (Jason.Care@melroseplc.net) immediately and inform them that there is a suspected breach and request that they contact you as soon as possible by telephone to discuss this further.

27.2 Upon the discovery of a personal data breach, a security breach management plan must be put in place and acted upon, incorporating the following steps:

27.2.1 A team of individuals must be assembled immediately by the legal team to investigate the cause and seriousness of the personal data breach;

27.2.2 We must determine who needs to be made aware of the personal data breach, whether the data can be recovered and/or if the damage can be limited in any way;

27.2.3 We must assess the risks of the personal data breach causing damage to the Melrose Group, the individuals concerned themselves and other third parties;

27.2.4 We must consider whether the authorities, affected individuals themselves and the wider public need to be notified / informed of the breach, depending on the seriousness of the personal data breach and applicable law; and

27.2.5 Following resolution of the breach, we must evaluate the identification and causes of the personal data breach as well as the response and amend any deficient security, procedures and policies accordingly.

### 28. REGISTRATION WITH REGULATORS

28.1 Local law may require that any collection of personal data be notified to the local regulators, although exemptions are often available (differing from country to country) in relation to fairly standard uses of data which are considered not to be problematic.

28.2 There are also sometimes requirements to notify the regulator if personal data is transferred outside a country (for example, within Europe) to another country which does not afford similar protection to the data. This will depend on local law.

## 29. PENALTIES AND CONSEQUENCES

29.1 Breach of data protection law has consequences. Any failure to comply with this policy puts the Melrose Group at risk of breaching data protection law. Precise sanctions will differ from country-to-country but could include:

29.1.1 the imposition of fines by regulators (under the GDPR there are potential fines of up to EUR 20 million, approximately £18 million or $24 million, or 4% of worldwide annual turnover, whichever is higher);

29.1.2 criminal sanctions through the courts; or

29.1.3 civil action by data subjects or those representing them (such as works councils or unions or plaintiffs' attorneys through class action lawsuits);

29.2 There is also of course the possibility of adverse publicity in relation to such issues, such as a breach of the security of the data.

29.3 It is therefore very important that all employees adhere to this policy. Any breach of this policy will be taken seriously and may result in disciplinary action.

## PART 3 – KEY TRENDS AND DEVELOPMENTS

*The introduction of the EU General Data Protection Regulation (the **"GDPR"**) made ensuring compliance with data protection and privacy rules an essential part of everyday business. As the number of countries and jurisdictions with data protection and privacy legislation has been on the rise, global businesses have been required to navigate broadening international landscape of legal and regulatory compliance to manage the risk associated with processing personal data, transferring it across borders and keeping it secure. This factsheet outlines some key trends and developments in this area.*

- **Increase in the number of data protection and privacy laws and their enforcement**

Since the GDPR came into force in May 2018, a number of jurisdictions, sometimes inspired by the GDPR, updated or began the process of updating their data protection laws. Notably, the Californian Consumer Privacy Act (the **"CCPA"**) and the Brazilian General Data Protection Law (the **"LGPD"**) have both come into effect this year. This trend is expected to continue in the coming months / years, driven by concerns of individual citizens over how their private data is being used by global businesses as well as governmental authorities, and the concerns of governments that sensitive data on their citizens might be misused by malicious actors.

With data protection regulators empowered to issue large fines for breaches of data protection laws, there is an expectation that the stepped up enforcement action will continue especially in the priority areas identified by the regulators (such as investigating cyber breaches and monitoring intrusive or disruptive technologies). Hand-in-hand with regulatory enforcement comes the rise of private litigation for breaches of privacy legislation, including the proliferation of class (collective) actions for large-scale data breaches.

- **Data protection trends in the United States**

In the US, the most significant privacy-related development in the last couple of years has been the passage of the CCPA and its implementing regulations. The CCPA is considered to be the most sweeping privacy law in the United States. It applies to companies that collect personal data from California residents and provides those individuals with certain rights to their personal data, including but not limited to the right to know and access and the right to delete. It also imposes corresponding obligations on businesses, such as the obligation to provide a notice at collection and to provide a privacy policy.

Although the CCPA only came into effect this year, there is already a ballot initiative for a proposed law to replace the CCPA. The California Privacy Rights Act (the **"CPRA"**) will be on the November ballot in California, and based on polls, it is highly likely to pass. If it passes, CPRA will provide additional rights to California consumers (such as the right to limit the use of sensitive personal data and the right to correct) and also impose additional obligations on businesses.

Numerous other states have proposed consumer privacy laws but none as broad as the CCPA has passed yet. (The few laws that have passed have been very limited in scope.) Some of the proposed laws have been similar to the CCPA and others have been more similar to the GDPR. In addition, a few federal consumer privacy laws have been proposed, but none has passed yet either. However, it is likely a matter of time before more consumer privacy laws are passed in the United States.

Aside from the trend regarding state consumer privacy laws, other recent trends include the expansion of the scope of or requirements under state data breach notification laws and the passage of laws imposing specific (and sometimes detailed) security requirements and other obligations on certain types of companies, such as data brokers, manufacturers of Internet-connected devices, and financial institutions.

- **Restrictions on international data flows on the rise**

Data localisation laws have been on the rise over the past few years. For example, China and Russia have passed laws requiring data about their residents to be stored in that country and transferred internationally only if strict requirements in the local privacy laws are met. Similarly, the GDPR requires that any transfers of personal data out of the European Economic Area (the **"EEA"**) are prohibited unless they meet specific requirements in the GDPR.

The Court of Justice of the European Union complicated international transfers of personal data from the EEA when it declared in July 2020 that the EU-US Privacy Shield used by many businesses to enable transfers of personal data to the US is invalid. The court also stated that for transfers of personal data from the EEA to a country not recognised by the European Commission as offering adequate protection, any party exporting personal data and the party receiving the data must conduct a case-by-case assessment to determine whether the transfer complies with the GDPR. While we await more guidance from the regulators, it is expected that this requirement to assess international data transfers will increase the burden on compliance and data protection teams over the coming months.

At the end of the Brexit transition period, transfers of personal data from the EEA to the UK will also have to comply with the specific GDPR requirements for international data transfers. Unless the European Commission recognises the UK as offering an adequate level of data protection before the end of the Brexit transition period, business will have to ensure that they have arrangements in place to continue transfers of personal data from the EEA to the UK.

Another trend is the diversion of interests between the US and China in relation to trade and national security, and the effect the tensions are already having and are likely to have on international data flows between the two countries, as well as globally.

- **The impact of COVID-19 on data protection and privacy**

COVID-19 has had a significant impact on data protection in the workplace and it is expected that this will continue for the rest of the year. Firstly, businesses have been required to adapt to working from home while mitigating the cybersecurity risk of remote working. On return to work, businesses have been required to start collecting additional personal data from their employees and visitors to keep their workforce safe and assist public authorities with COVID-19 contact tracing efforts. It will be important for businesses to continue monitoring the latest guidance from national governments and regulators in relation to what data should (and should not be) collected in the context of the pandemic, how long it should be retained for and how individuals should be informed about this. It is also advisable that businesses monitor announcements from national security agencies to help mitigate the risk associated with COVID-19-related cyberattacks.

- **Encouraging data sharing of non-personal data**

While in Europe the sharing of personal data is subject to strict privacy requirements, the sharing of non-personal data by businesses has increasingly been seen by governments as a possible driving force of modern economies which can fuel innovation.

In September 2020, the UK Government published a National Data Strategy which not only seeks to improve data use in government, but also open data in different sectors to drive innovation in a responsible way. Similarly, the European Commission supports the creation of common European data spaces, for example, for the manufacturing and mobility sectors to encourage companies to share their data based upon voluntary agreements. Both initiatives provide the Melrose Group with an opportunity to combine its own data with open data from the government and other businesses to drive innovation.

**KEY RESOURCES**

*Data protection*

- The UK Information Commissioner's Office
  https://ico.org.uk/

- The European Data Protection Board
  https://edpb.europa.eu/edpb_en

- Office of the Attorney General, California Department of Justice
  https://oag.ca.gov/privacy/ccpa

*Data strategies:*

- The UK National Data Strategy
  https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy

- A European Strategy for Data
  https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy