DATA PROTECTION POLICY

A. THE DATA PROTECTION POLICY

1. POLICY STATEMENT

1.1 Individuals have rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information 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 Brush and it is the responsibility of the directors of each such company to ensure that it is deployed within their local business. The General Counsel is responsible and accountable for incorporating this policy into local regulations and procedures to ensure compliance.

1.4 In Europe, Brush is exposed to potential fines of up to EUR20 million (currently approximately £18 million or $25 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the General Data Protection Regulation ("GDPR").

1.5 All company employees, contracts, agency staff and other personnel[1] 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 or on a computer or other media, is subject to certain legal safeguards. Legal obligations to which we are subject impose restrictions on how we may use that information. Where personal data has been collected or processed in the EEA by us or third parties, or where personal data about data subjects in the EEA has been collected or processed by us or third parties from outside the EEA in the course of delivering goods or services to such data subjects, or monitoring their behaviour (for example, with CCTV), in the EEA, we must comply with applicable European data protection laws (such as the Data Protection Act 1998 in the UK and, from 25 May 2018, the GDPR) when we process it (including where we transfer that personal data to other companies in the Melrose Group or third parties). Where personal information is being used by

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

us outside Europe, we must comply with the laws that apply to the use of personal information in those countries.

2.3 This policy has been approved by the Melrose Board. It may be amended at any time by the issuing of a replacement policy.

3. ENSURING COMPLIANCE WITH THIS POLICY

3.1 The company's General Counsel is responsible for ensuring compliance with this policy and is contactable by email at Ben.Hewitson@Brush.Eu.

3.2 Any questions or concerns about the operation of this policy should be referred in the first instance to your General Counsel. If you consider that the policy has not been followed in respect of personal data (whether about yourself or others) you should raise the matter with your line manager or your General Counsel.

4. DEFINITION OF DATA PROTECTION TERMS

4.1 **IN THIS POLICY, WE USE THE FOLLOWING TERMINOLOGY:**

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 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 who can be identified from that data (or from that data and other information in our possession on 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 securities personal data (see definition below).

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 loss, or unauthorised access, disclosure or acquisition, of personal 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 obtaining, recording 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 information about a person's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;

- physical or mental health conditions, or sexual life or sexual orientation;
- personal data, biometric or genetic data; and
- about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings.

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

B. EUROPEAN REQUIREMENTS: HANDLING PERSONAL DATA THAT HAS BEEN PROCESSED IN THE EUROPEAN UNION

5. THE FUNDAMENTAL EUROPEAN DATA PROTECTION PRINCIPLES

5.1 This Section B applies where we process personal data in the European Union or where we have received personal data from a party (such as another member of the Melrose Group or a third party) in the European Union under a data transfer agreement (see section 16 below) or we have received personal data from an individual in the European Union where we are offering him goods or services or monitoring his 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 are:

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 A requirement here is to ensure that data subjects know that data is being processed by the company and for what specified lawful purpose. Almost always this will be obvious from context and that will often suffice (depending on local European 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 the company's activities are:

6.3.1 that the data subject has consented to the processing,

6.3.2 the processing is necessary for the company 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 that the processing is necessary for a legitimate interest of the company or the party to whom the data is disclosed where that interest is not overridden because the processes prejudices the interests or fundamental rights and freedoms of the data subject(s). The purposes for which we process personal data for legitimate interests needs 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 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 your General Counsel 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 Melrose Group's data 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 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 retention policy that applies to your business. This includes required third parties to delete such 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**

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 data held about them by a data controller;

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

12.1.3 the right to ask to have inaccurate 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 data or to complete incomplete 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 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 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:

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 information is always considered confidential).

13.3.3 Methods of disposal. Paper documents should be shredded. Memory sticks, CD-ROMs, etc should be 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 system ("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 the company's 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.

14. CUSTOMER RELATIONSHIP MANAGEMENT SYSTEMS

14.1 It is important to remember when using any CRM tool that individuals (including employees and customer and supplier representatives) have rights under data protection laws throughout Europe and the rest of the world, including (often) the right to access data about them 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 company if the relevant data subject were to become aware of it. If there is an issue about an individual which others in the company 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 express consent would be needed in many offices.

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, the company 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 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 your general counsel 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 transfer restrictions; 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 EUROPEAN ECONOMIC AREA: ENSURING ADEQUATE PROTECTION

16.1 Organisations that collect and otherwise process personal data inside the European Union 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 European Economic Area ("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 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 EEA, that company can only do so if one of the following condition applies:

16.2.1 the recipient is located in a country which the European Commission has decided offers adequate protection (as of February 2018, these countries are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Jersey, the Isle of Man, Israel, New Zealand, Switzerland and Uruguay);

16.2.2 if that recipient agrees to enter into a standard form data transfer agreement approved by the European Commission for this purpose called the standard contractual clauses or other appropriate safeguards are in place, such as the recipient is subject to an approved code of conduct or framework (for example, US-EU Priory Shield);

16.2.3 the data subject has provided 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 1998 or, from 25 May 2018, the GDPR.

16.3 Our companies in the EEA must not transfer personal data to an entity which is located in a country outside 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. Where personal data is to be transferred to a member of the Melrose Group outside the EEA it will generally be possible to effect the transfer because we have in place intra group data transfer agreements to protect the personal data. Where we receive or access personal data on behalf of our non-EEA companies from members of the Melrose Group located inside the EEA or from third parties in the EEA that have entered into data transfer agreements with us, we must ensure that we process that personal data in a way that complies with the European data protection requirements described in part A and B of this policy.

17. PROVIDING INFORMATION 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 their line manager or General Counsel 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 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 data will be transferred outside of the EEA the requirement set out in Section 16, with respect to cross-border transfers must be met).

18. CLOSE CIRCUIT TELEVISION

18.1 The company may wish to install Close Circuit Television ("CCTV") surveillance on its European premises. When it does so, it should be clear about the reasons for installation: for example, whether it is as a security measure or alternatively as a measure for monitoring company employees. A privacy impact assessment may need to be completed to ensure that the company

complies with its data protection obligations. Please speak to your General Counsel for further details about how to complete this.

18.2 The company 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 The company 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 surveyed 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 the company receives a request (for example, from law enforcement agencies) in relation to disclosure of any images made, section 16 above will apply.

18.6 The company should 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 The company must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The company is responsible for, and must be able to demonstrate, compliance with the data protection principles. The company 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 presents 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 company personnel on 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 company must maintain a record of training attendance by its personnel; and

19.1.4 testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, 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 The company 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 detail set out above together with appropriate data flows.

21. TRAINING AND AUDIT

21.1 The company is required to ensure all personnel have undergone adequate training to enable them to comply with data privacy laws. The company must also test our systems and processes to assess compliance.

21.2 The company will periodically review the systems and processes under its 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 The company is 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. You 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 The company 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 General Counsel 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 data, for example:

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

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

23.2.3 derived or inferred 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 The company does 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 the company's data collection or engagement with 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 If the company identifies business activities or data collection activities in the United States that are subject to specific regulatory oversight, then the company will review regulations and relevant enforcement actions to clarify its legal obligations.

26. STATE LAWS

26.1 The majority of U.S. states have established data breach notification or data security laws or regulations that impose their own distinct obligations on U.S. entities. Where the company is subject to these laws as a result of its activities in particular jurisdictions or with regard to the data of citizens from those jurisdictions, it will review legislation and regulations to clarify its legal obligations.

26.2 As a general matter, many of these laws require notification to customers, state officials, and law enforcement in the event of a data breach of a delineated size.

26.3 If you identify a data breach involving U.S. information, please contact your General Counsel or Hollie Cope-Jones (hollie.cope-jones@melroseplc.net) immediately to determine any necessary compliance obligations.

D. GENERAL REQUIREMENTS

27. SECURITY BREACHES RELATING TO PERSONAL INFORMATION

27.1 If you suspect that a personal data breach has occurred, please contact your General Counsel and Hollie Cope-Jones (hollie.cope-jones@melroseplc.net) immediately and inform them of the suspected breach.

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 General Counsel to investigate the cause and seriousness of the personal data breach;

27.2.2 The company 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 The company 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 The company 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, the company 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 company 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 EUR20 million, approximately £18million or

$25 million, or 4% of Global 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);

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.