EM NORMANDIE UK LTD

PRIVACY STANDARD

Dated : 07/2020

Contents

CLAUSE

EM Normandie UK Ltd is committed to ensuring the protection of personal data collected in the course of its activities, and to comply with the applicable laws and regulation regarding the use of Personal Data, including the General Data Protection Regulation (GDPR).

The aim of this policy is to ensure there are appropriate policies and procedures in place to ensure that EM Normandie UK Ltd complies with its legal obligations.

1. INTERPRETATION

1.1 Definitions:

"Automated Decision-Making (ADM)" when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

"Automated Processing" any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

"Company name" EM Normandie UK Limited

"Company Personnel" all employees, workers, contractors, agency workers, consultants, directors, members and others.

"Consent" agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

"Controller" the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

"Criminal Convictions Data" means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

"Data Subject" a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

"Data Privacy Impact Assessment (DPIA)" tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

"Data Processor" the person or organisation that Processes Personal Data on behalf of the Controller.

"Data Protection Officer (DPO)" the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance.

"EEA" the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

"Data Protection Legislation" all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation

((EU) 2016/679), the Data Protection Act 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended.

"Personal Data" any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

"Personal Data Breach" 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 Data is a Personal Data Breach.

"Privacy by Design" implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

"Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies" separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

"Processing or Process" any activity that involves the use of Personal 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 transmitting or transferring Personal Data to third parties.

"Pseudonymisation or Pseudonymised" replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

"Related Policies" the Company's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data.

"Special Categories of Personal Data" information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2. INTRODUCTION

2.1 This Privacy Standard sets out how EM Normandie UK Ltd ("we", "our", "us", "the Company") handle the Personal Data of our students, suppliers, Company Personnel and other third parties.

2.2 This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present Company Personnel, students, or supplier contacts, shareholders, website users or any other Data Subject.

2.3 This Privacy Standard applies to all Company Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal

Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you for the Company to comply with Data Protection Legislation. Your compliance with this Privacy Standard is mandatory. Related Policies are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies. Any breach of this Privacy Standard may result in disciplinary action up to and including dismissal.

2.4 Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Privacy Standard or otherwise then you must comply with the Related Policies.

2.5 This Privacy Standard (together with Related Policies) is an internal document and cannot be shared with third parties or regulators without prior authorisation from the DPO.

3. SCOPE

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the Company and our operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 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 GDPR.

3.2 All Company Personnel who decide which Personal Data is collected, and how and why they are collected and processed are responsible for ensuring all Company Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure that compliance.

3.3 The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Olivier GROS-DUBOIS, Executive Management, +33 2 32 92 59 78, dpo@em-normandie.fr

3.4 Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company) (see paragraph 5.1);

(b) if you need to rely on Consent (see paragraph 6);

(c) if you need to draft Privacy Notices (see paragraph 7);

(d) if you are unsure about the retention period for the Personal Data being Processed (see paragraph 11);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see paragraph 12.1);

(f) if there has been a Personal Data Breach (paragraph 13);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see paragraph15);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 16);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see paragraph 20) or plan to use Personal Data for purposes other than what it was collected for;

(j) if you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see paragraph 2121);

(k) if you need help complying with Data Protection Legislation when carrying out direct marketing activities (see paragraph 22); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see paragraph 14).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

(b) collected only for specified, explicit and legitimate purposes (Purpose Limitation);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

(d) accurate and where necessary kept up to date (Accuracy);

(e) not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

(g) not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

(h) made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests; or

(e) to pursue our legitimate interests provided our interests are not overridden by the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

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

6. CONSENT

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity

are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters. A request for Consent must be put in writing and must be intelligible, easily accessible, and set out in clear and simple terms. Consent should be freely given,

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented or if the Consent was obtained some time ago and the Data Subject cannot be reasonably expected to remember giving his or her Consent, unless there is another lawful basis for processing the data.

When processing Special Category Data, we will usually rely on a legal basis for processing other than Consent if possible.

You will need to evidence Consent captured and keep records of all Consents up to date and in accordance with Related Policies so that the Company can demonstrate compliance with Consent requirements.

7. TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The GDPR 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. The information must be provided through appropriate Privacy Notices which must be in writing, concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

If you are collecting Personal Data from Data Subjects, directly or indirectly and including for human resources or employment purposes, then you must provide Data Subjects with a Privacy Notice in accordance with our Related Policies. The Privacy Notice should inform Data Subjects of the following:

- the identity and contact details of the Company as Data Controller
- the purpose for which Personal Data is collected
- the contact details of the DPO
- the grounds for processing, and if applicable the legitimate interest pursued;
- the retention period or the criteria for determining the retention period;
- if applicable, the persons (or category of persons) that the Personal Data will be sent to;
- the Data Subject rights;
- the possibility of complaining to the Information Commissioner's Office;
- if applicable, the existence of a Data Transfer outside the EEA and the associated rights;
- whether the Personal Data must be collected by law or contract;
- whether the Personal Data must be collected for the performance of a contract;
- whether there is an obligation for the Data Subject to give the Personal Data;
- the consequences of not providing the Personal Data;
- the right to withdraw Consent if processing is carried out on the grounds of Consent;
- the existence of any Automated Decision-Making and relevant information relating to the same;
- the existence of any further Processing for any other purpose and relevant information relating to the same.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the GDPR after collecting the data (where reasonably practicable), within a month of collecting, or when first communicating with the Data Subject and specify the source of the information and whether it is publicly available or not.

8. PURPOSE LIMITATION

8.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

8.2 You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

9. DATA MINIMISATION

9.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

9.2 You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

9.3 You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

9.4 You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

10. ACCURACY

10.1 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

10.2 You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11. STORAGE LIMITATION

11.1 Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

11.2 The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

11.3 You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

11.4 You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records

retention schedules and policies. This includes requiring third parties to delete that data where applicable.

11.5 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.

12. SECURITY INTEGRITY AND CONFIDENTIALITY

12.1 Protecting Personal Data

Appropriate technical and organisational measures must be put in place by the Data Controller in order to ensure the security of Personal Data, and prevent any unauthorised access, taking into account current technologies and the loss, destruction or damage that may result from unlawful Processing.

The Company's collection, use, processing, transfer, retention, sharing and destruction of Personal Data requires EM Normandie UK Ltd to take reasonable and efficient organisational and technical measures in order to:

- Prevent unauthorised persons from accessing the IT systems to process or use Personal Data (access control);

- Ensure that only authorised persons can access Personal Data, such access to be limited to the purpose for which the Personal Data is being processed. These persons must safeguard the confidentiality of the Personal Data to which they have access.

- Ensure that persons who are authorised to use a data Processing system only have access to the data they are authorised to access, and that Personal Data cannot be read, copied, altered or deleted without authorisation during the Processing, use and after saving (access control, need to know principle).

- Ensure that Personal Data cannot be read, copied, altered or deleted without authorisation during transport, electronic transfer or saving on storage media, and that it is possible to check and control the persons who transfer Personal Data with data transfer tools (disclosure control).

- Ensure that it is possible to control and check whether Personal Data have been added, altered or deleted from the data Processing systems, and if so by whom (entry control).

- Ensure that Personal Data processed on behalf of a third party is processed in strict compliance with the instructions of the Data Controller (task control).

- Ensure that Personal Data is protected against accidental destruction or loss (availability control).

- Ensure that Personal Data collected for different purposes can be processed separately.

- Ensure that the anonymization of Personal Data is in place where required by local laws in order to Process the data.

You must identify the risks to the fundamental rights and freedoms of those who are affected by the Processing before determining the security and confidentiality measures which are appropriate to reduce such risks. If there is a high risk for the private lives of Data Subjects, you must carry out a Data Privacy Impact Assessment to determine which security and confidentiality measures are required to reduce such risk. To this end, you must refer to the internal GDPR Policy which includes the procedure for such risk assessments.

The level of security measures necessary for the protection of Personal Data will depend on the nature of the data and the purpose of Processing.

13. REPORTING A PERSONAL DATA BREACH

The GDPR requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches (the DPO**)**. You should preserve all evidence relating to the potential Personal Data Breach.

14. SHARING PERSONAL DATA

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers, if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) 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;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross-border transfer restrictions; and

(e) a fully executed written contract that contains GDPR-approved third party clauses has been obtained.

In addition, any contract with a third party with whom we share Personal Data shall address the following:

- Clearly defined responsibilities.
- Property of the Personal Data.
- Details regarding the Processing (purpose, duration, nature, type of Personal Data and Data Subjects).
- International transfers of Personal Data.
- Use of sub-contractors.
- Policies relating to Data Subject rights.
- Retention and deletion of Personal Data following termination of the contract.
- Security and Confidentiality obligations.
- Possibility of an Audit by Data Controller.
- Policies relating to Data Breach.

15. TRANSFER LIMITATION

15.1 The GDPR restricts data transfers to countries outside the EEA to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

15.2 In any event, a written agreement should be entered into with any Data Processor outside the EEA, with contractual provisions requiring them to put in place adequate

technical and organisational security measures to ensure the security of the Personal Data.

15.3 You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subject's rights and freedoms (the list of EC decisions is available on the EC website, which should be checked regularly for updated information: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en);

(b) appropriate safeguards are in place such as), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

16. DATA SUBJECT'S RIGHTS AND REQUESTS

16.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) 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;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) object to decisions based solely on Automated Processing, including profiling (ADM);

(i) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(j) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(k) make a complaint to the supervisory authority; and

(l) 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.

16.2 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).

16.3 You must immediately forward any Data Subject request you receive to the DPO.

17. ACCOUNTABILITY

17.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

17.2 The Company must have and continue to have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines or Privacy Notices;

(d) regularly training Company Personnel on the GDPR, this Privacy Standard, Related Policies and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

You must complete and update records for each instance of Processing, and specify the purpose of such Processing. You must also retain evidence of compliance with laws and regulations relating to the Processing recorded. You are responsible for ensuring compliance with this Policy and Related Policies, and must ensure that you are in a position to demonstrate that all technical and organisational measures were taken to limit the risk to the private lives of Data Subjects.

18. RECORD KEEPING

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

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Controller and the DPO, 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 for the different categories of Personal Data and a description of the security measures in place. To create the records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. TRAINING AND AUDIT

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

20. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

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.

You must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high-risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and ADM;
- large-scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
- large-scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

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

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Special Categories of Personal Data or Criminal Convictions Data are being processed, then grounds (b) or (c) will not be allowed but the Special Categories of Personal Data and Criminal Convictions Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

22. DIRECT MARKETING

We are subject to certain rules and privacy laws when marketing to our students or alumni.

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 contacts 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.

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.

A Data Subject's objection to direct marketing must be promptly honoured. If a contact 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.

23. DATA MANAGEMENT

23.1 Responsibilities of the DPO

The DPO safeguards the compliance of Personal Data Processing within the Company. Their main role is to ensure that EM Normandie UK Ltd is and remains compliant with the legal framework relating to Personal Data (General Data Protection Regulation). In this context, the DPO has confidentiality obligations and observes the strict confidentiality of information, procedures, uses, complaints and litigation that they should become aware as part of their DPO duties.

Ensuring compliance of EM Normandie UK Ltd Processing activities

- Ensuring Processing records are up to date.
- Following new projects and ensure impact assessments are carried out on new Processing activities.
- Ensuring that contracts with third parties and Data Processors are compliant.
- Being aware of legal developments to identify any requires updates to this Policy or Related Policies.
- Carrying out training and raising awareness of Company Personnel obligations relating to Personal Data Processing.
- Checking the application of different Data Protection policies and applying them to different processes: HR, Marketing, IT,..
- Regular reporting to management on work carried out and work remaining to be done, and any risks identified relating to Personal Data.
- Supervise internal annual audits to ensure compliance of Processing activities.

Being the point of contact for the Data Protection Authority

- Notifying the Data Protection Authority as required

EM Normandie UK Ltd's obligations towards the DPO

- Ensuring the DPO is consulted on any question relating to Personal Data, or any new proposed Personal Data Processing activity.
- Giving the DPO adequate resources for them to carry out their functions (material or financial resources).

- Enabling the DPO to access Personal Data and Processing activities carried out by EM Normandie UK Ltd.
- Safeguarding the independence of the DPO and ensuring they receive no instructions in carrying out their duties.
- Ensuring the DPO is free to organise and decide how to carry out their duties.
- Enabling the DPO to deal with board level management.
- Ensuring the DPO is not given other duties which may create a conflict of interests.
- Ensuring the DPO is not personally liable for EM Normandie UK Ltd's compliance with Personal Data laws and regulations.

23.2 Responsibilities of all Company Personnel

With regards to the DPO, you must:

- Give the DPO's contact details when collecting Personal Data (as per your obligations under this Policy).
- (for managers) inform their teams of the appointment of the DPO, of their name and contact details.
- Carry out risk assessments for each Processing. Where there is a significant risk, carry out a Data Privacy Impact Assessment and involved the DPO in the assessment of all new projects.
- Take into account Data Protection obligations before each new project.
- Implement Privacy by Design and Privacy by Default in each new project.
- If applicable, document and justify in writing why the DPO's advice was not followed.
- Reply to any information requested by the DPO relating to matters having an impact on privacy.
- Enable the DPO to access documents relating to Personal Data Processing and related procedures.
- Inform the DPO of any new Processing activity such that it can be included in the Processing records.

24. CHANGES TO THIS PRIVACY STANDARD

24.1 We keep this Privacy Standard under regular review. This version was last updated in September 2019.

24.2 This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Company operates.