1. Introduction

Data Protection legislation within the United Kingdom defines in law, principles for the processing and protection of personal data. Non-compliance with relevant legislation, either as a Company or as an individual, is an offence that could lead to criminal prosecution. In order to adhere to data protection principles and to protect information received from our customers, business partners and our employees, it is essential that we take steps to ensure that data in our possession is kept safe and secure.

It is important to recognise that many of the GDPR's main concepts and principles are much the same as those in the Data Protection Act 1998 (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so we have to do some things for the first time and some things differently.

The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in this policy will require Vandercom to review our approach to governance and how we manage data protection as a company issue. The regulatory framework will be referred to as the "legislation" or similar in anticipation of the enactment of the Data Protection Bill and associated regulations.

Vandercom is working to comply with all relevant data protection legislation by undertaking improvements, including but not limited to, delivering training to all employees, conducting audits against the requirements of relevant legislation, undertaking Data Privacy Impact Assessments (DPIAs) and updating our relevant contracts.

2. Purpose and scope

The purpose of this policy is to inform employees, and those engaged on behalf of Vandercom, of their obligations. It is also intended to be distributed to customers, potential customers and interested parties to advise them of our understanding and approach to data protection legislation. Data protection legislation applies to 'controllers' and 'processors'. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller. Where Vandercom are a processor, the legislation places specific legal obligations on us, for example, we are required to maintain records of personal data and processing activities. We will also have potential legal liability if we are responsible for a breach. However, if Vandercom is a controller, we are not relieved of our obligations where a processor is involved – the legislation places further obligations on you to ensure your contracts with processors comply. The legislation applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

3. Definition of personal data

‘Personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way we collect information about people.

The legislation applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised can fall within the scope of the legislation depending on how difficult it is to attribute the pseudonym to a particular individual. The legislation refers to sensitive personal data as “special categories of personal data”. The special categories specifically includes health data, trade union membership, sexual orientations as well as genetic and biometric data where processed to uniquely identify an Individual.

4. Roles and responsibilities of the Data Controller

Vandercom has appointed Timea Rozsahegyi, as Data Controller for Vandercom to monitors internal compliance, informs and supervises data protection obligations, and act as a contact point for data subjects and the supervisory authority.

5. Staff responsibilities

As an employee, you are responsible for the safeguarding of any data that you have access to, irrespective of the format. Employees are reminded that your contract of employment and relevant HR policies both contain confidentiality obligations, obligating every employee to assume responsibility for the protection of information (data) accessed whilst discharging their duties. Any breach of this mandatory obligation may lead to formal action up to and including dismissal following the full disciplinary procedure. All data should be securely stored in the specific areas that you are instructed to store it in, to ensure that it is available to only authorised users across the business and to support activities in place to prevent data being lost or stolen. Access to any restricted area is limited to authorised staff that have the necessary clearance to support business operation or supporting infrastructure.

You must follow the full data protection checks, as laid out in your training, with a customer before speaking to them about or taking any actions upon their account. You must not provide anyone with information about a customer’s account unless they have passed the data protection checks.

Should any other member of staff ask you to provide them with any data, (whether it be about one (or more) customer(s), the business, or an employees(s)), then you should assess if the release of that data is justifiable and proportionate for business purposes in the context of the requesting party’s job role. If you are unsure at any point, please speak to your line manager. Any filing procedures, (for both paper and electronic documents) that form part of your job role should be followed at all times. All employees should ensure that all visitors to the office or other unauthorised persons are unable to view customer, business or employee data whether held on paper documents or information displayed on PC monitors.

It is every employees’ responsibility to undertake annual data protection training as communicated. Employees should also, where appropriate, consider the data

protection principles when commencing a project or undertaking significant changes to the handling of personal data. They should also embed the principle of “privacy by design” in their work.

5.1. Management responsibilities

New staff should be carefully coached and trained before being allowed access to personal or sensitive data, they should be fully aware of how to store, handle and protect all data. Access to files containing sensitive or confidential data should be monitored by supervisors and managers on a regular basis to ensure that data is being handled and stored appropriately.

Regular checks shall be carried out to ensure that employees are not leaving sensitive data on their desks, or viewable on their PC’s when they are away from their desk.

All staff are to contact the Data Controller for advice before any personal data is sent outside of the EU or EEA.

If staff are unsure of their obligations, they should seek advice from the Data Controller.

6. Data Subject Rights

Data subjects have rights under data protection legislation. For example, the right to rectification provides that if organisations hold inaccurate data, the data subject can request that it is corrected within a period of no longer than thirty days. Often, how we deal with data subject rights will go through our business as usual processes. Other rights include the right for data to be erased, the right to access data (often referred to as a Subject Access Request), right to object and to restrict processing. There are also rights in respect of data portability and automated decision making, including profiling. If someone asks to exercise one of these rights, you must make contact with the Data Controller immediately for advice. If a customer asks for a contact email address in relation to data protection they should be advised to contact timea@vandercom.com

7. Six principles of the data protection legislation (including GDPR updates)

There are six principles in the legislation and Vandercom must ensure that personal data is:
a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the legislation in order to safeguard the rights and freedoms of individuals; and

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. Retention

Please ensure you have read and understood our control of records procedure. All employees are under a duty to comply with the principles of data protection legislation which includes an obligation to retain data no longer than is necessary.

9. Security controls

Vandercom undertake penetration testing to ensure it environment is secure. For more information on employee responsibilities please refer to the Vandercom Privacy Policy. Vandercom also embeds data protection, security and confidentiality clause in our supplier contracts.

10. Incident management

The legislation introduces a duty on all organisations to report certain types of personal data breach to the Data Controller. You must do this within 24 hours of becoming aware of the breach, where feasible. For these reasons employees must report suspected or actual data breaches without delay using the incident reporting procedure outlined on the Security procedures. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Vandercom must also inform those individuals without undue delay. Managers should ensure that where they are responsible for systems or infrastructure that they have robust breach detection, investigation and reporting procedures are in place. Vandercom's Data Controller maintains a record of any personal data breaches, regardless of whether you are required to notify the Information Commissioner's Office.

11. Data Protection Impact Assessment (DPIA)

A data protection impact assessment (DPIA) is a process to help Vandercom identify and minimise the data protection risks. Vandercom employees must engage with the Data Controller who will undertake a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Our Data Controller may engage with specialist security partners to support the DPIA process. Vandercom should also undertake a DPIA for any other major project which requires the processing of personal data. Vandercom DPIAs: describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks. The Data Controller will then assess the level of risk and the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. Employees should consult the Data Controller if they believe a DPIA is required. If you identify a high risk and you cannot mitigate that risk, you must consult the Data Controller before starting the processing.