General Data Protection Regulation (GDPR) Statement

Vancols Ltd GDPR Assessment 2018

Introduction

GDPR sets out and legislates how Vancols and Rotary Portraits (Europe) collects, stores, and handles personal information – across digital, paper, and any other type of media. The GDPR legislation comes into effect on the 25th of May 2018. Prior to the introduction of the GDPR – Vancols Ltd fully supported and subscribed to the outgoing Data Protection Act. Rotary Portraits will be referred to in this document as Vancols / Vancols Ltd.

Vancols Information Commissioners Office (ICO) registration number is Z6069453.

For the ICO website & GDPR information, please follow this link: https://ico.org.uk/

Assessment

Vancols Ltd has conducted GDPR assessments and has determined that Vancols Ltd obtains and processes data.

Vancols Ltd has determined that Vancols Ltd process data in the following way.

A data controller and processor of its own employee data.

1. A data controller and processor of third party data.
2. A data controller or processor of data such as activity relating to direct marketing for School Services, and customers, including photography and marketing services (brochures / websites / signage & general marketing)

Vancols work with the following data:

- Employees.
- Customers.
- General Business Contacts.
- Suppliers.

This can also include other businesses or individuals. These are categorised as 1) Consent 2) Legitimate Business interest.

Vancols subscribe to the GDPR regulations. By doing so, we ensure that we:

- Comply with the data protection law and follow good practice.
- Protect the rights of staff, customers and partners.
- Vancols are open about how it stores and processes individuals' data.
- Vancols protects itself from the risks of a data breach.

By doing so, we ensure that we adhere to the six principles of GDPR, as detailed under Article 5.

Article 5 of the GDPR sets out the six principles of data protection. These principles are the foundation of the GDPR and require 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 GDPR 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.”

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-dpr/principles/

Vancols Responsibilities under GDPR

Vancols GDPR statement applies to:

- Vancols Head Office
- Vancols Staff – Full time / Part time / Seasonal
- Any individual or supplier working for Vancols on instruction

Vancols GDPR statement covers the following data we process – where an individual can be identified from the data:

- Names
- Email addresses
- Postal addresses
- Telephone numbers
- Detail required to process payments
- Photographs
- Any other data which could be used to identify an individual

Responsibilities

Vancols Ltd has a requirement to ensure data is collected, stored and handled appropriately, and staff have GDPR training to facilitate the correct usage of data.

Staff member who process or access data are required to adhere to the General Data Protection Regulation 2018 principles.

The Board of Directors is responsible for ensuring that Vancols Ltd meets its legal obligations.

The Data Protection Officers (DPO's), **David Blackwell** and **Mark Misquitta** are responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging GDPR training and advice for the people covered by this policy.
- Handling data protection / GDPR questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Vancols Ltd holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The IT Manager **Stuart Robins**, in conjunction with the DPO's, is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The Marketing Manager, **David Blackwell**, is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

Vancols Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data is not to be shared informally. When access to confidential information is required, employees can request it from their managers.
- Vancols Ltd will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- Robust passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of. If physical data medium, shredded.
- Employees can request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection and GDPR.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Manager or Data Protection Officer. Vancols uses personal data to allow ordering, management, and delivery of our photographic and marketing services.

- When not required, the paper or files are kept in a locked drawer or filing cabinet.
- Employees make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts are shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts using appropriate digital security.
- Data is protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these are kept locked away securely when not being used. CD and DVD images are securely disposed of when finished with.
- Data is only stored on designated drives and servers, which are on site in the UK.
- Laptops are never left in vehicles overnight.
- Data is backed up frequently. Those backups are tested regularly, in line with the company's standard backup procedures.
- Data is never saved directly to mobile devices like tablets or smart phones.
- All servers and computers containing data are protected by approved security measures.

Data Use

- When working with personal data, employees ensure the screens of their computers are always locked when left unattended.
- Personal data is not shared unnecessarily.
- Data must be protected before being transferred electronically.
- Personal data is never transferred outside of the European Economic Area.
- Vancols do not share any data with third parties.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data Accuracy

The law requires Vancols Ltd to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Vancols Ltd should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Staff - Photographers

Photographers laptops are encrypted, and secure password protected. Images on the laptop are encrypted. Photographers are DBS checked which is available on request.

Staff - Sales Managers

Vancols (DBS checked) Sales Managers use our contact database. This is accessed remotely. No contact data is stored on laptops.

- The laptops used are password protected.
- Our database is password protected.
- Data used is typical school contact information.
- The data on our CRM systems is checked against the Department of Education's most up to date UK school list regularly – to ensure data is as up to date as possible.

Head Office and Processing

Our office and processing department are located at our secure head office site, covered by CCTV inside and out, and alarmed. Passcode entry for access. Only approved staff can access the building and data. Visitors cannot get on site without being allowed in by a member of staff via locked front gate. Computers are password protected. Physical data is shredded once finished with. All Vancols images are produced internally and then packed by our own internal packing department within processing. Images posted are sent white label with no other identifying data other than name and address of recipient.

Customer Orders

Vancols uses its own in-house developed software to facilitate and process online orders. Every image is stored securely on an enclosed password and firewall protected network. Customers can also order by post or through a back to school process where parents return the order via the school.

Online, customers can only access images using a secure individual photocode provided to them. Customer must set up a personal password protected account and input the unique photocode to access their image. Images cannot be accessed without a unique code.

Vancols website use Secure Trading and PayPal who deal with the complete process of handling the card payments. All payments are taken through Secure Trading and PayPal encrypted processes. This transactional data is not stored.

CCTV

Vancols uses CCTV externally and internally. Recordings are held in a 5-day loop with appropriate security applied.

Payments

Payments can be cash, cheque, or card. Appropriate security is applied. Details are processed then securely destroyed.

Data Storage

Photographers Data is stored on laptop for one school term.

This data is backed up on digitally secure on-site storage. Only authorised office and lab staff have access to the data. SIMS or AI data is returned to the school for deletion or is securely disposed of once used.

Photos are stored for varying lengths of time depending on the usage. Images can be stored for around ten years as Vancols finds that parents often purchase older photos, where they have forgotten to order at the time, or to purchase images of their child when they were younger. Often schools ask for previous year groups heads shots for their records.

General school contact information is refreshed against the Department of Education’s most recent school listing or when we identify a change through normal business operation.

Security

Security is subject to ongoing review across both physical on-site security, and digital security. Customer facing digital security is tested using what is known as a penetration test. Vancols also review against what is the current best practice digital security methods (both hardware and software), as these change over time.

Subject Access Requests (SAR)

All individuals who are the subject of personal data held by Vancols Limited are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its GDPR obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer (DPO) david.blackwell@vancols.com, or mark@vancols.com. The DPO can supply a standard request form, although individuals do not have to use this.

The DPO will aim to provide the relevant data within 28 days.

The DPO will always verify the identity of anyone making a subject access request before handing over any information.

Vancols will delete the information on request by the individual in entirety.

Vancols Ltd do not charge for subject access requests.

Disclosing Data for other reasons

In certain circumstances, the General Data Protection Regulation 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Vancols Ltd will disclose the requested data. However, the Directors will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Vancols Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used.
- How to exercise their rights under GDPR.