GDPR STATEMENT

POL-GDPR-VC-V1.2-2018 Issue 1.2 23rd April 2018

VideoCentric's handling of data with reference to GDPR requirements, effective from May 2018 onwards, is split into two – **EMPLOYEE DATA** and **CUSTOMER DATA**. This document distinguishes between the two, what data is held or may be held, how concerns are managed and how often the processes will be reviewed.

EMPLOYEES

Every staff member of VideoCentric has been made aware of GDPR and what it means to them, our Company and our customers

Each employee has the right to request that personal data be deleted if deemed unimportant to their employment with the Company. Such deletions, if agreed, shall be carried out within 72 hours, or if a valid reason for non-deletion is stated, the employee shall be informed in writing, within 5 days of the initial request.

Information held about staff members is not shared with anyone except Company Directors. Although a GDPR Officer may be appointed who is not a Director, the said GPDR Officer will not have access to personnel data held.

Data held regarding employees includes or may include:

- full name,
- address of permanent residence,
- personal email,
- business email,
- home phone number,
- mobile phone number,
- social media identifiers,
- IP addresses,
- URL identifiers,
- ISDN number,
- salary details,

- NI Number,
- next of kin,
- passport details,
- driving licence details,
- criminal convictions,
- driving offences,
- date of birth,
- place of birth,
- bank account details,
- child care scheme details,
- children's details (only those required to fulfil child care scheme),
- holiday entitlement & usage records,
- training records,
- expense claim records,
- cloud service usage,
- business travel records

The security of the above records will be strictly monitored by Company Directors and reviewed not less than once every six months.

Employees will be informed within 72 hours, if a breach of data has been suspected or confirmed. Further notifications will be made each 24 hours (business days only), outlining the risk, the potential impact and the actions to minimise risk and implement corrective action, until the problem has been dealt with and the case is closed by the Company Directors.

The above list may be updated from time to time by re-issuing this GDPR statement. It is the responsibility of each employee to review it with respect to their personal situation and to approach a Company Director in writing if an objection is to be raised.

CUSTOMERS

VideoCentric's GDPR Statement is non-confidential and may be communicated by any member of staff. Additionally, any intermediate partner, authorised reseller, project manager, customer agent or supplier may, upon request, receive the same statement and have their own details treated in exactly the same way as our end-customers. Hereon, each will all be considered as customers.

Each customer has the right to request that personal data be deleted at any time. Such deletions, if agreed, shall be carried out within 72 hours, or if a valid reason for non-deletion is stated, the customer shall be informed in writing, within 5 days of the initial request.

VideoCentric's policy is to contract with **businesses only (B2B)** and therefore consumer sales (B2C) do not form part of its strategy or marketing plan. As of 25th May 2018, any records thought to be B2C records, originating from accounts such as Hotmail, Gmail, Yahoo or BTinternet domains or similar, will have been deleted from VideoCentric's database altogether. All new web-initiated enquiries from the GDPR date onwards will contain a "B2B only" instruction, and an "opt-in" box for

any communication other than the first one. Email footers of sales and marketing staff will also contain an “opt-out” box as will the web-site’s “contact us” page.

Information retained securely by VideoCentric, **will never be sold** and will only be used for VideoCentric’s own marketing purposes where there is a legitimate interest in respect of products already purchased, or solutions enquired about, or related systems and services that may be of real potential business benefit moving forward. In all cases VideoCentric will maintain a legitimate reason for why each record exists and will behave in such a way as to demonstrate a relevant and appropriate relationship.

In conducting its B2B business, VideoCentric needs to share information with its manufacturers, importers, trade distributors, service providers, courier/delivery companies, legal organisations, crime enforcement organisations, business development partners, consultants, 3rd-party support & services partners, cloud onboarding & training partners, our resellers, geographic agents and finance/leasing organisations. While VideoCentric will take the necessary steps to point out the importance of their own GDPR compliance in dealings with VideoCentric customer data, VideoCentric itself cannot offer any guarantees on their behalves and will not be held legally liable for any breaches by those partners. VideoCentric will maintain a log of each of its suppliers/partners GDPR statements and will periodically review whether it should continue to trade with any partners who do not meet VideoCentric’s own ethical standards.

VideoCentric is acutely aware of the nuisance factor of unwanted or overly frequent marketing messages but from time-to-time will make contact with customers and potential customers though courtesy, helpfulness maintaining communication and building better business relationships.

Data held regarding customers includes or may include:

- customer name,
- web-site,
- primary & secondary contact names,
- addresses of each site concerned,
- general company and personal emails & phone numbers,
- mobile phone numbers,
- social media identifiers,
- IP addresses,
- URL identifiers,
- ISDN numbers,
- bank account details (but NOT credit card details, or card security codes)
- cloud usage records,
- business travel records,
- Return on Investment (RoI) calculations,
- network quality statistics,
- performance graphs
- communications histories.

The security of the above records will be strictly monitored by Company Directors and reviewed not less than once every six months.

Credit & Debit Card Details are collected by phone for the sole purpose of fulfilling individual purchases relating to a quotation. Up to three authorised individuals (one in Sales, one in Operations, one in Accounts) are approved to carry out such transactions and it is Company policy to destroy by shredding, any handwritten notes within 10 minutes of each transaction with nothing stored electronically for future use. Website transactions are via approved and secure 3rd party payment brokers such as Paypal, Stripe and Worldpay and never will a customer be asked to supply details by email under any circumstances.

Customers will be informed within 72 hours, if a breach of data has been suspected or confirmed. Further notifications will be made each 24 hours (business days only), outlining the risk, the potential impact and the actions to minimise risk and implement corrective action, until the problem has been dealt with and the case is closed by the Company Directors.

GDPR - A process of compliance with continuous improvement

GDPR (General Data Protection Regulation) is a European-wide set of legal requirements for strict enforcement by all organisations in the UK and beyond. It will protect the right to privacy for every EU resident and on 25th May 2018, it will replace the 1995 EU Data Protection Directive (95/46/EC). Any organisation, including VideoCentric and every one of its staff, have an obligation to comply. This document provides an awareness of the data held for existing employees who must sign to confirm awareness. New employees will be trained on GDPR requirements and will be required to sign this document before being able to access or process any customer data.

Some confusion still exists in terms of how GDPR will be monitored, reviewed and enforced and it is clear that new requirements will emerge over time, moving the goal posts yet again, including the EU's new ePrivacy Regulation (ePR). Strong fines do exist for organisations who fail to comply or are negligent in putting processes into place where shortfalls are recognised. This statement is therefore to be considered as a snap-shot of VideoCentric's current intention which shall be open to comments for improvement by employees, customers, agents, partners and management in accordance with the Law and good business practice.

GDPR STATEMENT (Issue 1.2) - SIGNATURE PAGE

Each existing and new Employee is obliged to sign this page confirming that he/she has understood VideoCentric's Statement on GDPR and wishes to be bound by it.

Customers may optionally sign this page which will be countersigned by a Director of VideoCentric or an appointed GDPR Officer confirming that we are happy to consider this as a formal agreement between our organisations.

…….	……..	……..
Employee (mandatory)	Print Name	Date
…….	……..	……..
Customer (optional)	Print Name	Date
…….	……..	……..
Director or GDPR Officer	Print Name	Date

Note that this GDPR Statement is a live document and up-issues will remain accessible via www.videocentric.co.uk although re-signing won't standardly be requested by VideoCentric. A customer may provide a written request for re-signature at any time and this will be actioned by VideoCentric within 3 business days.

---End of Document POL-GDPR-VC-V1.2----