Data Exchange Policy

Integrity Communications Group has a legal obligation and a reputational interest in ensuring that the exchange of data, including personal and sensitive data, between itself and its customers and suppliers is compliant with the requirements of the UK General Data Protection Legislation (GDPR) and all other applicable data protection laws.

This policy document sets out the basis on which Integrity Communications Group will exchange data with its trading partners and describes the procedures that will be followed. It refers to the associated Data Protection Policy and to the Integrity Communications Group Terms and Conditions of Sale and Terms and Conditions of Purchase. These documents may be accessed via the Integrity Communications Group website (www.integritycommunicationsgroup.com)

Purpose

The purpose of this policy is to explain to all the parties involved how Integrity Communications Group will manage data exchange, placing this in context with the specific GDPR principles that are relevant to this process. These principles are:

- That personal data is protected by design and by default. Organisations are required to implement technical and organisational measures to demonstrate that data protection is considered and treated as an integral aspect of their processing activities

- Organisations must ensure that personal data is protected against unauthorised or unlawful processing; and must ensure that technical and organisational measures have been taken to protect against accidental loss, destruction or damage.

The method that individuals use to exchange data with trading partners has a profound effect on the security of the data; the risks include data being intercepted in transit, being stored in an insecure location after receipt, and being accidently or purposefully re-distributed and made accessible to unauthorised persons.

With heightened risk comes greater exposure to legal liability, punitive fines and reputational damage.

Integrity Communications Group is determined to ensure that its own employees and its customers and suppliers are aware of these risks; and that appropriate data exchange practices are followed.

Scope

This policy includes the exchange of data:

- Within the Integrity Communications Group business; between individuals within a trading division and between trading divisions.

- From Integrity Communications Group to customers, suppliers and other third-party organisations.

- From customers, suppliers and other third-party organisations to Integrity Communications Group.

The policy is specifically targeted at exchanges of data that involve confidential, personal or sensitive information.

A distinction is made between that and the interchange of everyday information that is typically passed in telephone conversations and plain-text emails; this policy does not seek to address the handling of non-confidential, non-personal or non-sensitive information.

The important criteria in the context of this policy is the definition of personal data which is specifically described by Article 4 (1) of GDPR as:

"… any information relating to an identified or identifiable natural person ('data subject')…'

So personal data includes anything that indicates the identity of an individual; this is commonly a name or address, but may also include other locational data, as well as account references, identification codes (such as passport and national insurance numbers) and even online identifiers such as the IP addresses of personal computers.

By contrast, the definition of confidential data is rather imprecise; this will include information, which may be financial, related to businesses and other organisations, and does not fall within the scope of GDPR. When exchanging this class of data employees and external parties must use their own discretion in determining the level of protection to apply to the transfer.

General

All existing and new employees of Integrity Communications Group will be given an induction into the principles of GDPR and how these relate to the operational processes that are associated with their role within the business.

Employees and their line managers must ensure that they have received the appropriate technical training and are able to implement the measures described in this policy to ensure the secure exchange of data.

When necessary, the Integrity Communications Group employee who is liaising with an external sending or receiving party must ensure that guidance is given to the other party to ensure that the objectives of this policy are satisfied.

Personal data must not be transferred outside the European Union unless appropriate safeguards are in place (as set out in the current data protection legislation) or unless the transfer is otherwise permitted under the current data protection legislation.

If the method of data exchange fails to conform to this policy then the Integrity Communications Group employee must raise a Security Incident Report and submit this to the Information Security Forum.

Employees should be aware that under GDPR the risk of financial penalties and reputational damage are so severe that if they are found to be in breach of the policy they are liable to be disciplined in accordance with the Integrity Communications Group disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in the immediate termination of employment.

Data Exchange Methods

Exchanging data via email is inherently weak, it therefore must not, under any circumstances, be used as a method for exchanging personal data.

Non-personal data may be exchanged via email, but the sender must consider and use their judgement to decide whether the data requires encryption.

To encrypt a file a suitable software application, such as 7Zip, WinZip, SecureZip etc, should be used.

If a file containing non-personal data is encrypted and is exchanged by email, the encryption password must not then be advised by email (not even in a separate message). A password should be advised by telephone or text message, or otherwise pre-agreed, so that it cannot be easily matched to the file.

Passwords should be complex, with a minimum of 8 characters and using at least three of the following four types: upper case letters, lower case letters, numeric and special characters.

The problems associated with email include:

The sender may forget to apply encryption to safeguard attachments.
The sender may advise the encryption password in an insecure manner.
The email advising an encryption password may sit in an Inbox alongside the file.
The sender may misdirect the email to an unintended recipient.
The sent email may be intercepted in transit.

- The received email and file may never be deleted from the email system.
- The received email may be forwarded to unauthorised recipients.

Should an external party choose to email a file containing personal data to an Integrity Communications Group employee, the employee is not permitted to retain the file within the bounds of their email account, neither are they permitted to forward the email and file to any other person. The file must be saved to a designated network folder (where appropriate access controls will be in place), and the file attachment removed from the email (via the Remove Attachment function).

Online file sharing sites, such as Dropbox, Google Drive, WeTransfer and others, must not be used to exchange data, even at a customer or suppliers behest. This is because it is not practical to audit the use of these publicly available sites, and the risk of losing control is therefore unacceptable.

Where there is a need to exchange large files containing non-personal data, the functionality provided by Microsoft OneDrive through Integrity Communications Group’s Office365 account may be used. Each requirement should be discussed in advance and managed by the Integrity Communications Group IT Department.

Integrity Communications Group stipulates in its Terms and Conditions that personal data may only be exchanged via its secure SFTP / FTPS site.

This applies to all three directions of data exchange, that is: between Integrity Communications Group employees and divisions; from external parties to Integrity Communications Group; and from Integrity Communications Group to external parties.

The Integrity Communications Group SFTP / FTPS site and its user access credentials for employees, customers and suppliers are managed by authorised staff in the IT Department.

The web front-end to the SFTP / FTPS site supports the enforcement of complex password construction, password ageing and disabling of account access if unused for a specified period, and it also provides password change and forgotten password functionality.

Folders on the SFTP / FTPS server may be set up with upload permissions (for customers), download permissions (for suppliers) or, if necessary, with both.

The subsequent internal transfer of received files from the SFTP / FTPS server to the network folders used to support data processing and production activities is a fully automated process. This contrasts with all other data exchange methods where manual involvement, with its inherent risks, is necessary.

All activity on the SFTP / FTPS site is automatically logged and is monitored by the IT Department.

Integrity Communications Group reserves the right to wholly delete from all its systems any received file containing personal data that was not exchanged in compliance with this policy.

Liability

Integrity Communications Group will not be liable for any loss, unauthorised disclosure or other data breach if an external party exchanges data in a manner that fails to comply with this policy.

Integrity Communications Group will not be liable for any loss, unauthorised disclosure or other data breach if an external party fails to exercise control over the access credentials to the SFTP / FTPS site.

Further details are available in the Integrity Communications Group documents:

- Terms and Conditions of Sale
- Terms and Conditions of Purchase