Westcoast Ltd's GDPR Policy Statement

GDPR

General Data Protection Regulation (GDPR) - All of Westcoast's policies and procedures adhere to the current data protection act (1998), but will align to the GDPR when it takes effect on May 25th 2018.

What is GDPR?

The GDPR, General Data Protection Regulation, is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union.

Key Steps that Westcoast have undertaken

Westcoast are committed to high standards of information security, privacy and transparency. Westcoast will comply with applicable GDPR regulations when they take effect in 2018 and our ongoing preparations for this includes:

AWARENESS: **Briefing all staff so they are aware of their obligations in relation to the handling of personal data (with the associated risks to the business) and what needs to happen to get GDPR compliant**

SPONSORSHIP: **Appointed a Board sponsor who supports and oversees all internal GDPR work programs**

STAFFING: **Appointed a working group responsible for GDPR who meet weekly to discuss progress on agreed actions**

LEGAL OPINION: **Translated the GDPR into deliverables & functionalities so that Westcoast can align their compliance objectives, and mark progress against tasks as they are completed**.

PERSONAL DATA DISCOVERY: **Conducting a Personally Identifiable Information (PII) location / format / security assessment across all data using departmental representatives**

PROGRAMME PREPAREDNESS: **Assessment of exposure & potential mitigations (Risk Based Approach)**

POLICY GAP ANALYSIS: **Review and update of existing data protection policies, training, privacy notices etc. to be ready in time for the May 2018 deadline**

For more information contact: **gdpr@westcoast.co.uk**

TECHNICAL GAP ANALYSIS: **Where IT solutions can accelerate GDPR "effectiveness" acquiring & installing these IT solutions and services**

SECURITY CERTIFICATIONS & IMPROVEMENTS: **Continued commitment to security, tools and data protection across the business (Achieve security certifications to emphasise our data security controls)**

CUSTOMERS: **Aligning to our commitments as a Data Processor and adhering to all mandatory requirements set out under the GDPR.**

In addition to the above commitments, like many organisations Westcoast are making a whole host of technical, organisational, contractual and process-led changes to ensure we are meeting the requirements of the new Regulation.

Detailed Q & A Responses

Part 1 - Data Protection & Information Security

Do Westcoast have a documented Data Protection Policy?

Yes – we have a documented Data Protection Policy which obliges our organisation and all its employees and/or contractors to comply with the latest Data Protection legislation? (i.e. GDPR)

How often is our Data Protection Policy reviewed?

It is reviewed annually

Who is responsible for the circulation, maintenance and development of our Data Protection Policy?

The Privacy Compliance Officer and Head of Information Security are jointly responsible for the maintenance and development of our Data Protection Policies, but the circulation is done via a wider compliance team.

Is our Data Protection Policy readily available to all users? If yes, please state where it is located?

It is located on our local Intranet site and accessible by all staff

Do Westcoast have a documented Information Security Policy?

Yes – we have a documented Information Security Policy, which obliges our organisation and all its employees and/or contractors to comply with Data Protection legislation. Additionally we have a Privacy Policy signed by all staff, which informs staff how we process their personal data

How often is our Information Security Policy reviewed?

It is reviewed annually

Who is responsible for the circulation, maintenance and development of our Information Security Policy?

The Head of Information Security is responsible for the maintenance and development of our Information Security Policy.

Is our Information Security Policy readily available to all users? If yes, please state where it is located?

It is located on our local Intranet site

Part 2: Internal Security Controls

Describe the technological security measures you have in place to safeguard personal data.

We adopt a layered approach to security, with a number of differing levels of safeguards in place to protect personal data. This is aligned to the different levels of risk that we have assigned to the personal data we store and process, and therefore the security measures we deploy can vary.

Do you hold Information management security standards accreditations?

Yes – Westcoast are a Cyber Essentials certified organisation.

Certification Number is 2795237340353555. The certification is valid until March 14th 2019.

Have your security policies, procedures and standards been reviewed and assessed by a qualified independent organisation?

Yes - they have been through a review and assessment by a qualified independent organisation as part of the Cyber Essentials certification process.

Has your security infrastructure been reviewed and tested by a qualified independent organisation?

Yes – we have external CHECK and CREST certified independent security specialists that test our external security perimeter and infrastructure as part of certification and annual penetration testing programs.

How are Westcoast systems protected against newly discovered vulnerabilities or threats?

We have our own vulnerability scanning toolset that we use to manage scheduled scans.

Are security audits performed?

We have an internal audit team who are responsible for auditing general IT controls.

Does the Westcoast maintain and will maintain adequate Records of Processing Activities regarding the personal data it processes?

Yes we maintain records of processing, which includes legal basis for processing personal data

Have Westcoast audited their internal systems for those that hold personal data?

Yes, all systems have been subject to an audit by the technical teams

Part 3: Environmental, Physical and Organisational Security

Where Westcoast staff have access to the personal data of customers, tenants and/or employees, is there a confidentiality clause in their employment contracts?

Yes, there is a reference to confidentiality in our employment contract AND additionally we have a Privacy Policy signed by all staff

Do we offer regular data protection training to all our staff?

This is currently being formalised into our new Learning Management Solution, which will go Live in May 2018, and become an annual requirement. At present, our internal training team delivers data protection training in the form of classroom sessions and workshops.

Do we offer additional data protection training to any of our staff (i.e. those working with any sensitive personal data)

All training requirements are assessed by the Training and Learning Management team at Westcoast Ltd. Where applicable additional training in areas pertaining to data protection can be facilitated if deemed necessary

Do we maintain a record of any data protection training provided to our staff?

This is currently being formalised into our new Learning Management Solution, which will enable us to deliver this using an automated tool.

Do we have a documented procedure for dealing with members of staff who breach any of our data protection policies?

Yes – we have a Breach Assessment and Action Plan along with a Data Breach Incident Plan

Describe what physical security measures we have in place for unauthorised access to any of our work space (i.e. key fob/ID card)?

Dependant on the site we will have either key fob access or picture id access control in place.

What measures do we have in place to prevent staff from installing potentially malicious software?

All requests for additional software have to go through a formal approval by both line manager and IT. The request then is logged on our Service Desk portal and is assigned to an analyst to install after approval. Standard users do not have rights to install ANY software themselves.

How do Westcoast protect information that is taken offsite?

We provide clear guidance in our Staff Handbook around what data can be taken off site and what should not leave our premises. There is also clear guidance around personal data usage and obtaining the correct approvals to access personal data.

Do Westcoast have any sub-processor contracts?

Yes we do have sub-processor contracts, and these include a provision in relation to our respective data protection obligations

Do Westcoast engage sub-processors in the provision of services? If so, do we have a GDPR-compliant process for engaging sub-processors?

We have a formalised approval process that we go through when reviewing sub-processor compliance with the GDPR. Where we engage sub-processors in the provision of services, we have sent out GDPR processor agreements that need to be signed up to ensure onward processing compliance.

Part 4: Data Breaches & Governance

Do you have a documented procedure which details a plan of action in the event of a data breach of data protection legislation?

Yes – We have a Data Breach Management Policy.

Do Westcoast have a procedure in place to ensure notification is made without delay of a data breach concerning the personal data of customers and/or employees?

Yes – we have procedures in place to ensure the ICO is notified within the required 72 hr timeframe if a reportable data breach concerning the personal data of our customers were to occur. This is included in Breach Assessment and Action Plan.

After a data breach, are our policies and procedures reviewed to determine if any modifications need to be made?

If a data breach was to occur, then yes we would review our procedures and make modifications if lessons learned required us to do so.

Do we have a Data Breach Register?

Yes we have an ICO approved Breach Register that is updated in the event of a data breach

Have Westcoast breached the Data Protection Act 1998 in the last 3 years where the breach was reported to the affected data subjects? If yes, please provide details and explain what action was taken.

No

Have Westcoast appointed, or will we appoint a Data Protection Officer?

Westcoast have a Privacy Compliance Officer that assumes certain responsibilities within our internal governance framework in relation to data protection.

If Westcoast are not established within the EU, have we appointed an EU representative?

Westcoast are established in the EU, once we leave the EU we will still adhere to all the same standards

How will Westcoast assist organisations to ensure that an individual can exercise their rights under the GDPR with respect to their personal data?

Westcoast have a documented Subject Access Request Process which meets the requirements of the GDPR. We will therefore assist using formalised ICO approved guidelines if an individual requests to exercise their rights under the GDPR with respect to their personal data.

Part 5: Data Retention and Disposal

Do we have a Data Retention policy?

Yes we have a Data Retention Policy in place which reflects the additional amendments required for GDPR. As part of an ongoing revision to this policy we are incorporating the alignment of retention and destruction dates for all document types.

Where is our data stored and backed up (Supplier/Location/Country)

The majority of our organisational data is stored at the SRS Data Centre (our contracted DC provider) based in Wales, UK which is in the EEA

Describe how our data is permanently deleted once it is no longer required in order for you to fulfil your contractual obligations.

Data will be securely destroyed as per contractual obligations and our destruction obligations.

Do you have a Destruction of Media Policy?

Destruction of data guidelines and advisory around how often data should be purged is incorporated in our Data Retention and Destruction Policy.