Introduction

Welcome to The Icon Group's statement on GDPR and Data Security. The General Data Protection Regulation (GDPR) is a European Union Regulation that has been designed to strengthen and unify Data Protection within the EU. The GDPR came into effect on 25 May 2018. The GDPR harmonises Data Protection practices across the EU and emphasises accountability, security and transparency by data controllers and processors, while at the same time strengthening and standardising the right of European citizens to privacy of their personal data. The Icon Group ensures to comply with the latest GDPR regulations by updating and adapting current procedures as required.

Commitment

The Icon Group are committed to ensuring the security and protection of the personal information that the company processes, and to provide a compliant and consistent approach to data protection.

The Icon Group ensures the security of Personal Data at all times is in line with the Data Protection Acts 1998 and 2003 and guidance issued by the Data Protection Commissioner of Ireland. We are compliant under the EU General Data Protection Regulation (GDPR) at all times.

The Icon Group has a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. Icon is committed to our customers and the protection of our customers' data.

We are registered Data Processors with the Data Protection Commission. We require our staff to commit to three levels of confidentiality when signing a contract of employment:

- To respect the confidentiality of the Client's data, systems and intellectual property
- To respect the confidentiality of the Applicant's data
- To respect the confidentiality of Icon's systems and work practices

We work to ISO 27001 standards and principles in managing data. We will always consider context in relation to data security to ensure that any aspects to data storage or movement that might be novel, unusual or have a vulnerability.

Our offices have controlled access by means of key card, where entry and exit times are recorded. This is augmented by video surveillance. Due to current circumstances related to COVID-19, all staff are currently required to work from home (WFH) and are implementing a clear desk policy.

The enforced change from an office based environment to WFH has not compromised our principles and procedures in terms of processing and managing data with confidentiality and care. We have implemented a number of procedures to ensure that Client (and other) data is secure and managed appropriately.

Outlined below are the principles and practices we at Icon use to ensure that our work is GDPR compliant and in line with the requirements outlined by the Commission for Data Protection.

The Icon Group operate by the following GDPR Principles:

Accountability
The Icon Group is committed to the principles of the GDPR by adopting the concept of 'data privacy by design' within our operational model. The company remains accountable by having detailed policies and systems in place as well as a Data Protection Officer to oversee our overall compliance to data protection regulations including the management of access rights requests. Our policies are regularly updated and reviewed, and our staff are periodically trained on data protection and security throughout the year.

Lawfulness, Fairness and Transparency
The Icon Group processes data with data subjects' interests in mind and ensure that employees approach processing activities with transparency to maintain fairness in what is done. This way the company can be sure that data is processed lawfully. The Icon Group has a robust process in place that allows us to deal efficiently with any access requests received.

Data Integrity and Confidentiality
The Icon Group holds data on secure systems, and operates to the level of IS027001. Information security and integrity is key to our operations. Our strict regulations ensure resources are protected from unauthorised viewing and other access, ensuring confidentiality. All information is protected from unauthorised changes to ensure that it is reliable and correct, guaranteeing data integrity. Any instances of potential data security issues are dealt with swiftly by our IT experts and are reported in full.

Data Minimisation and Data Storage
The Icon Group will not keep data for longer than is necessary and only keep data if there is a lawful basis which allows fair retention. When the company does need to remove data from our possession, we do so by using industry approved standards so the disposal or anonymisation is thoroughly compliant.

Data Accuracy
Keeping data accurate is very important to us and the Icon Group trains all staff members to ensure they are maintaining data to a high quality and with all the facts available. All employees pass a rigorous training programme to ensure the highest standards are obtained, with refresher courses regularly undertaken. The Icon Group implements a stringent quality control procedure across all projects, emphasising the importance of focusing on minute details to ensure accuracy and retain integrity in all data.

Purpose Limitation
The Icon Group uses the data obtained for a specific purpose. This means that data is not processed for any alternative reasons other than what the data was originally collected for. The tables below explain the company's stance on different operational areas of our business, so that you can easily see the standards we work by.
If you have any further queries about any topics raised in this document please contact our Data Protection Officer on contact@icon.ie for further assistance and clarity.

Physical Security of our Sites

Note: Due to current restrictions on travel and human interaction, all operations are currently conducted off site in a WFH capacity.

Buildings

Reception areas are staffed during working hours with door access control systems in place throughout the building. All entrances are monitored by CCTV including internal CCTV in the Icon Group's office. All staff must visibly wear a lanyard and an employee identification card at all times.

When required to work from the premises of a Client, Icon Group staff operate and adhere to the security codes of the Client. This includes but is not limited to the wearing of a lanyard, visible ID, controlled access points, door access controls, and operational desk policies.

Secure areas

Secure access areas are protected by entry controls in Icon Group working spaces to ensure only authorised staff can enter via an access control card. Access rights are removed when staff move roles and access rights are limited to necessary personnel required.

Systems Security

Software and Applications

Software and applications are managed through strict licensing and permissions.

The Icon Group uses bespoke custom built software where we can control the number of users at any point. Access for these secure systems is applied for when needed and removed when an employee ends their contract of employment with the company. All Icon Group software undergoes rigorous trials and examinations before being implemented.

The Icon Group uses commercial software systems for use on certain projects. These software are installed locally and all derived data is stored securely on encrypted hard drives or on our Google Cloud platform.

All PC security is continually monitored to ensure the latest updates to Windows and antivirus software are installed.

Network Access

Access to Google Drive is accessed via https secure internet browser.

Users who require access to external servers are required to change their passwords every 8 weeks. Previously used passwords are not permissible.

All access to external servers are controlled by the Client and we adhere to their security parameters at all times.

VPN Access

All remote access via remote working employees is secured by VPN log on technology. Users are unable to access the networks unless a secure VPN connection has been established.

Encryption

Downloading of files from external databases are only possible using encrypted keys. These keys are stored securely with limited access given to staff.

Testing
All new system testing is carried out using a secure development link, with updates and new software releases only being shared with a limited number of staff once secure testing has been completed. Software and applications go through an evaluation, testing and deployment protocol.

System Updates
The Icon Group updates systems at time appropriate intervals to ensure we are always using the most advanced technical and organisational tools available.

Data Back Ups
Specific data is backed up weekly and a data restore process has been tested. Measures are in place to ensure that the business can continue to function should a compromise occur. Performance monitoring and file integrity monitoring is in place to ensure our business continuity plan can take full effect.

Data may be backed up to physical media stored offsite at our secure data backup facility, secured with CCTV, physical locks and limited access controls.

Monitoring and testing
A standard build procedure ensures that all default admin and back door accounts are removed. The Icon Group has implemented an exit strategy to ensure all inactive accounts are deactivated, access to emails are removed and confidential data returned and deleted if required.

Regular network monitoring by the company's IT expert identifies any non-compliance to data loss from prevention controls.

Penetration testing at application and network level is carried out on a regular basis.

Cloud Providers
We may use cloud storage facilities for processing and storing data. We ensure that security is maintained through a strict permissions system which is monitored daily.

Google Cloud has a secure-by-design infrastructure built-in protection, and a global network that is used to protect information, identities, applications, and devices. Google encrypts data in transit between their facilities and at rest, ensuring that it can only be accessed by authorised roles and services with audited access to the encryption keys

All data resides in the EU or Ireland area and no data is transferred out of the EEA.

Cyber Security
All networks have firewalls, antivirus and malware protection in place which is deployed on all endpoints to detect, alert and neutralise any threats.

Any applications accessible from the internet are constantly safeguarded to prevent the existence and exploitation of web application vulnerabilities such as cross-scripting or SQL injection.

External connections are protected with resilient firewalls.

Firewalls and monitoring control and monitor traffic entering and leaving the organisation.

All Icon Group staff have received training on how to identify security threats and the “next step” protocols. All security threats are reported and investigated fully.

Data Breaches

Our procedures ensure that we have safeguards in place to identify, assess, investigate and report any personal data breach as early as possible.

All Icon Group employees have been trained in identifying potential data breaches and reporting them swiftly and accurately.

Operational procedures are in place to inform the Client(s) immediately of any data breaches pertaining to a compromise of their data.

International Data Transfers and Third-Party Disclosures

Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as binding rules, or standard data protection clauses for those countries without.

Project related data transfers occur only with the express written consent from the Client.

Third Party

All contractual IT security requirements are in place with any third parties we use which ensures the relationship remains subject to GDPR compliance.

Where necessary, our contract with them includes Data Processing Terms or terms are built into our products terms and conditions.

We also use alternative data protection safeguard mechanisms where appropriate in the form of standard contractual clauses where required.

Staff Security

All staff are screened prior to their engagement and interviews are face to face where possible.

All staff get an induction focused on data protection and all our staff’s CV statements and qualifications are checked for validity before the offer of employment can commence.

Staff access to data is restricted by the project to which they are contracted.

Each staff member is issued with an Employee Handbook which we regularly review and update where necessary.

We update our staff when additions and updates are made.

A restrictive covenant is signed by staff prior to employment and a confidentiality agreement is signed on the first day on employment.

All staff receive security training as part of their induction which is reinforced periodically during training sessions and presentations. Staff receive regular additional training on cyber security awareness.

Staff are expected to change their passwords regularly and we enforce complex password requirements.

When an employee leaves the business, all accounts and access is suspended immediately, blocking all access to our systems and buildings.

A clear desk policy is in place across the Icon Group and staff procedure is to lock screens when they are away from their desks for any period. WFH has not altered this policy; our staff security procedures are still enforced and monitored while WFH is in place.

We operate policies for data security for our remote and field workers so that integrity is always maintained.

Staff are not permitted to store any data via removable media (USB's) or on device hardware unless the removable media is encrypted and authorised by the Client(s).

Data Retention, Requests and Disposal

Data Retention

All data retention is handled in line with our retention policy. We are committed to taking a practical approach in line with legal, contractual and commercial requirements relating to the ownership, retention and disposal of information relating to our business activities within Ireland. The Icon Group will not keep data for longer than is necessary and only keep data if there is a lawful basis which allows fair retention.

Retained data may be the subject of audits by licensed supervisory bodies. The Icon Group has an obligation to comply with any supervisory or regulatory data protection body in relation to audits of retained data and information.

Data can be removed from cloud services and back up devices at the written request of the Client upon termination of services. Data can also be returned to the Client or amended at the Client's written request.

The deletion, amendment or return of data to the Client is contingent on EU laws which apply to the Icon Group.

Data Subject Access Requests

Article 15 of GDPR allows individuals the right to request a copy of any of their personal data which is being processed.

In the event that right of access is requested, the Client is notified if any relating data to the Client is included in any such request.

Once right of access has been established and the Client has been informed of the nature of the requests and related data concerned, the Icon Group have operating procedures in place to release pertinent data.

Data Disposal

As a company we have made a conscious effort to become more digitally focused and we steer away from paper records wherever possible.

Confidential waste bins are located on each floor for confidential paper waste and this is securely shredded before disposal.

We have a hardware disposal policy in place which ensures that all hardware is wiped before final destruction.

Queries and Complaints

The Icon Group has a dedicated representative who can be approached for any questions, comments and requests regarding this privacy policy or our Data Privacy Management System.

The Icon Group welcomes communication around our policies and practices and they can be directly contacted on the details below.

Phone number: +353 1 406 2568

The Icon Group, 123 Baggot St Lower, Dublin 2, Ireland, D02 YK29.

Data Protection Officer: contact@icon.ie

Additional Information

This version was last updated and reviewed in October 2020.
We regularly review and monitor regulatory guidance for any industry changes which may impact our business operations or your rights and freedoms.