DRIVE RESCUE

GDPR COMPLIANCE STATEMENT

Taking the Protection of your Personal or Organisation's Data Seriously

Introduction

Your data security is of the upmost priority to us. The **EU General Data Protection Regulation ("GDPR" or "Regulation")** came into force across the European Union on 25th May 2018 and brought with it the most important changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age. The twenty first century brings with it extensive use of technology with data spread across numerous devices, new conceptions of what constitutes personal data, and a massive increase in cross-border processing. The new Regulation aims to regularise data protection laws and processing across the EU; granting individuals stronger, more consistent rights to access and control their personal data.

This **Compliance Statement** highlights measures taken by **Drive Rescue** to comply with data protection requirements under the **GDPR**, the **Data Protection Act 2018, Irish ePrivacy Directive** and other relevant data protection laws and regulations. **Drive Rescue** is an IT consulting company providing advanced data recovery services in Ireland. Our clients comprise of individuals, businesses, organisations as well as government agencies. Our contact information is provided below.

Our Commitment to GDPR Compliance

As a data recovery company, **Drive Rescue** (hereafter "we", "our" or "us") understands that it may regularly be involved in retrieving and processing information containing personal data which is subject to GDPR data protection requirements. We are committed to ensuring the security, integrity, and confidentiality of the personal information that we retrieve and process, and to provide a compliant and consistent approach to data protection.

We have always had a strong and effective data protection program in place which complies with existing Ireland data and privacy laws and abides by Principles of Data Protection. However, we recognise our obligations in updating and expanding this program to meet GDPR compliance requirements, Ireland's Data Protection Act 2018, ePrivacy Regulations and other relevant data and privacy protection laws and directives.

Drive Rescue is devoted to safeguarding the personal data under its control and in developing a data protection approach that is effective, appropriate and that exhibits an understanding of, and appreciation for the GDPR. Our measures and goals for GDPR compliance have been summarised in this statement. This Statement also informs you of the creation and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and thorough compliance.

How we have complied with the GDPR

In our resolve to ensure a consistent level of data protection and security across our company and fully comply with the GDPR, we have implemented the following measures: -

Information Audit – To assure compliance with the GDPR, we have carried out a company-wide information audit aimed to identify, register, and structure the personal data that we hold and process. The audit has summarised clearly the categories of personal data that we have collected or obtained, sources of the data, the lawful grounds for processing, the purposes of processing, parties to whom such data may be disclosed as well as parties responsible for safeguarding such data.

Policies & Procedures – The Company has put in place several data protection policies and procedures needed to meet the requirements and standards of the GDPR and any relevant data protection laws. These include: -

- **Data Protection Policy** – We have overhauled our data protection policy and implemented a comprehensive policy and procedure document for data protection that meets the standards, principles and requirements of the GDPR and relevant data protection laws. Our data and security policy encompasses all aspects of collection, use, storage, structuring, transmission and disclosure of personal data. The Company has also put in place accountability and governance measures to ensure that we understand and carry out our obligations and responsibilities accordingly; with a focus on privacy by design and the rights of individuals.

- **Data Retention & Erasure Policy** – The Company has reviewed its data retention practices and consequently adopted personal data retention and erasure policy including a retention schedule that will govern the period that data and records will be retained. The schedule will also make sure that the Company meets GDPR's 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed in a lawful and transparent manner. We have put erasure procedures in place to meet the new 'Right to Erasure' obligations and are aware of when this and other data subject's rights apply along with limitations on this right, response timeframes and notification requirements. From time to time, the Company regularly purges and discards data in line with its data retention policy.

- **Data Breaches** – As part of the Company's eagerness to comply with data protection laws and the GDPR, we have adopted a data breach policy and procedures to ensure that we have safeguards and measures in place to identify, evaluate, probe, record, report, minimise and/or prevent any personal data breach at the earliest possible

time. Our procedures are strong and have been circulated to all employees, making them aware of the breach reporting obligations and steps to follow.

- **International Data Transfers & Third-Party Disclosures** – Drive Rescue recognises that transfers of personal data undergoing processing or intended for processing after transfer to a third country or an international organisation, must comply with data protection laws as well as Chapter 5 of the GDPR. We have put effective policies, procedures and protection measures in place to secure, encrypt and preserve the integrity of the personal data that is stored or transmitted outside the EU. Our procedures include a regular review of the destination countries to assess whether they provide an adequate level of protection, the implementation of provisions for binding corporate rules, the use of data processing agreements with third parties, as well as the use standard contractual clauses or approved codes of conduct for those countries. We perform comprehensive due diligence checks with all recipients of personal data to evaluate and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable. Third parties to whom we transfer data must also agree to comply with our policies and institute minimum security measures for the use, storage and disclosure of personal information. Our contracts with third parties also require indemnification to the Company in the event of unauthorised use or disclosure of information transferred by us.

- **Procedures for Subject Access Requests (SAR)** – The Company have established SAR procedures that complement our data protection and procedures policy. We have also revised our SAR procedures to accommodate the 30-day timeframe for handling subject requests for information. In the event of a subject access request, an extract of information processed by the Company shall be provided to the data subject free of charge. Our new procedures explain how to verify the data subject, what steps to take for processing an access request, what limitations apply and a guide of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

Legal Basis for Processing – The Company understands that in accordance with the GDPR, it can only process personal data under certain conditions and for specified and legitimate purposes. The company must therefore demonstrate the legal grounds it relies to process personal data. We have are reviewed all processing activities to identify the legal basis for processing of personal data and ensuring that each basis is appropriate for the activity it relates to.

Privacy Notice/Policy – We have revised our Privacy Policy to comply with the GDPR, ensuring that we explain clearly how and why we collect and use personal data and that all individuals whose personal information is processed are properly informed of their data rights, third parties to whom personal information is disclosed to and what safeguarding measures are in place to protect their information.

Obtaining Consent – we have revised our consent mechanisms for collecting personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, easy and intelligible ways to provide positive consent to us processing their information. We have developed rigorous processes for recording consent, making sure that we can demonstrate an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

Direct Marketing – we have revised the wording and processes for our direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe mechanism on all subsequent marketing materials.

Data Protection Impact Assessments (DPIA) – where we process personal data that entails considerable risk, large scale processing or sensitive data, we have developed and apply strict procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to moderate the risk posed to the rights of data subject(s).

Processor Agreements – where we use any third-party to process personal data on our behalf, we have drafted Data Processing Agreements and due diligence procedures for ensuring that third parties understand and meet GDPR obligations. These measures include initial and ongoing reviews of the service provided, specifying the necessity of the processing activity, and the technical and organisational measures in place and commitment to comply with the GDPR.

Special Categories Data - where we obtain and process any special category information (sensitive data), we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate legal basis. Where we rely on consent for processing, such consent must be explicit and verified by a signature, with the right to modify or remove consent being clearly indicated.

Data Subject Rights

In addition to the policies and procedures outlined above, we strive to ensure that individuals can enforce their data protection rights. On our website, we provide information regarding individual right to access any personal information that the Company processes about them. Individuals can request information about: -

- Personal data we hold about them;
- The purposes of the processing;
- The categories of personal data concerned;
- The recipients to whom the personal data has/will be disclosed;
- How long we intend to store personal data for;
- If we did not collect the data directly from them, information about the source;
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this;
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use;
- The right to lodge a complaint or seek legal remedy and who to contact in such instances.

Information Security & Technical and Organisational Measures

Drive Rescue takes the privacy and security of individuals and their personal information very seriously and we therefore take every reasonable precaution to protect and secure the personal data that we process. We have put strong information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction. We have also put in place several layers of security measures, including particularly standard commercial encryption, network security policy, password policy, pseudonymisation, the use of asset management programs, role-based access to personal data, penetration and vulnerability testing, intrusion detection systems, regular hardware back-ups, the use commercially available firewall and antivirus as well as monthly software and hardware updates.

GDPR Roles and Employees

To streamline compliance with GDPR, **Drive Rescue** has appointed Darragh Quinn as its Data Protection Officer (DPO) and has created a data privacy team to develop and implement its framework for complying with the new data protection Regulation. The team is responsible for promoting awareness of the GDPR across the company, assessing our GDPR readiness, identifying any compliance gaps, make recommendations and implement the new measures, policies, and procedures.

We understand that continuous employee awareness and understanding is vital to the full compliance of the GDPR. We have therefore involved our employees in our compliance plans. We have implemented an employee training program which has been provided to all employees prior and forms part of our induction and annual training program.

If you have any questions about our compliance for the GDPR, please contact our Data Protection Officer using the address below.

Data Protection Officer
Drive Rescue,
6-9 Trinity Street,
Dublin 2.

E: infoATdatarecoverydublin.ie
Website: www.datarecoverydublin.ie