Introduction
The EU General Data Protection Regulation ("GDPR") comes into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades.

Founded on the fundamentals of privacy by design and a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broad use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU, affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment
Opals Group ('we' or 'us' or 'our') are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection.

We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise the requirement and importance of updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

Opals Group are dedicated to safeguarding the personal information under our remit and to developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation.

Our preparation plans for the GDPR have been summarised in this statement and includes the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We are Preparing for the GDPR
Opals Group already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by 25th May 2018.
Our preparation includes:

- ***Data Audit*** - carrying out a company-wide data audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- ***Policies & Procedures*** - The revision and implementing of new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including:
    - Data Protection – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

- Data Retention & Erasure – we have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- Data Breaches – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possibility. Our procedures are robust and have been disseminated to all employees, who are aware of the reporting lines and steps to follow.
- International Data Transfers & Third-Party Disclosures – Opals Group does not currently store or transfers personal information outside the EU. Where this becomes a business requirement, we will develop robust procedures and safeguarding measures to secure, encrypt and maintain the integrity of the data. Our procedures will include a continual review of the countries with sufficient adequacy decisions; standard data protection clauses or approved codes of conduct for those countries without. We will carry out strict due diligence checks with all recipients of personal data to assess 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.
- Subject Access Request (SAR) – we have revised our SAR procedures to accommodate the revised 1-month timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- Legal Basis for Processing - we have reviewed all processing activities to identify the legal basis for processing and ensured that each basis is appropriate for the activity it relates to. Where applicable, we are also maintaining records of our processing activities, ensuring that our obligations under Article 30 of the GDPR are met.
- Privacy Notice – we have developed a Privacy Notice to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- Obtaining Consent - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence 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 – Whilst we do not carry out any Direct Marketing activity currently, should we do so, we will include clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- Data Protection Impact Assessments (DPIA) – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent 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 reduce the risk posed to the data subject(s).

- Processor Agreements – where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, Hosting etc), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- Special Categories Data - where we obtain and process any special category information, 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 Article 9(2) basis. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.
- Data Subject Rights - In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we have communicated directly with all "data Subjects" advising them of their rights and have provided easy to access information via our intranet of an individual's right to access any personal information that Opals Group processes about them and to request information about: -
    - What 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 your 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 judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

Opals Group takes the privacy and security of individuals and their personal information very seriously and are taking every reasonable measure and precaution to protect and secure the personal data that we process. We have dedicated information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including (in no particular order):

- Hardware Firewalls
- Software Firewalls
- Web Applications Firewalls
- Intrusion Prevention and Detection Systems
- Anti-Virus

- Remote and Local Security Scanning
- Data Encryption
- Secure Socket Layer
- Application Security Reviewing
- Penetration Testing
- Password Protection
- Denial Of Service Protection
- Secure storage locations for paperwork prior to scanning and shredding

GDPR Roles and Employees
Opals Group have designated Data Controller and Data Processor roles and have appointed a GDPR Working Group to develop and implement our roadmap for complying with the new data protection Regulation.

The Working Group are responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

Opals Group utilise a GDPR checklist designed by our Data Controller to assess each business activity, function and process and to ensure that we have a company-wide approach to meeting the new standards and requirements.
Opals Group understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program which will be provided to all employees prior to May 25th, 2018, and forms part of our induction and annual training program.