GDPR Compliance

The GDPR is the largest expansion of privacy laws in the EU in 20 years, and harmonizes all data privacy laws across Europe and the UK. This whitepaper covers the main impacts to institutions using StarRez to manage their operations.

Who does it apply to?

Most institutions will be affected by these changes. The laws apply to any institution doing business with EU and its citizens, such as accommodation providers accepting residents from those countries. The laws will be enforced from the 25th May 2018.

How is it enforced?

The maximum penalty for infringing these laws is the greater of €20 million or 4% of worldwide turnover, in addition to any action by the subjects to whom the data concerns. If an institution has a physical presence in the EU, GDPR fines can be enforced directly by any of the EU member states. If an institution has no physical presence in the EU, GDPR fines can be enforced by established International Law. In the US, this is additionally enabled by the mechanisms in the EU-US Privacy Shield agreement.

The UK will be implementing the GDPR regardless of Brexit. Only if it subsequently chooses not to join the European Economic Area (EEA) will the GDPR no longer apply. If this occurs, the UK will still need to implement equivalent protections to facilitate trade with the EU.

Key Points

- **Seeking Consent** – The GDPR establishes clear guidelines for what is considered 'consent' for a subject's data to be processed, and specifically identifies silence, pre-ticked boxes or inactivity as not meeting consent requirements.

- **Breach Notification** – National supervisory authorities must be informed of a data breach within 72 hours of the institution becoming aware. The affected subjects of that data breach must be informed as soon as reasonably practicable, if there is a high risk to them.

- **Right to Access** - An individual must be able to access any information being stored on them, and the institution is required to provide this free of charge, in a commonly accepted electronic format.

- **Right to be Forgotten** - Unless it is in the public interest for the subject's details to be retained, they must be erased when requested, unless they are legally required to be kept. There are limitations on this right, which each institution will have to seek advice on.

- **Privacy by Design** - The institution is required to put in place technical and organisational controls to protect privacy. This means applying common principles such as making information available only to those with a need to know, limiting access to the minimum required to perform a role, and other controls. The GDPR requires companies to be able to demonstrate this compliance, such as via externally audited standards like ISO27000, COBIT and SSAE-16.

- **Data Protection Officers (DPOs)** - This is a mandatory role required for any institution whose *'core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale'*, which would apply to any housing operation. DPOs must report to the highest level of management within the institution, and have expert knowledge on EU data protection law and practices.

More detail

The following provides additional detail on the key points in the GDPR, from an accommodation provider's point of view. For brevity's sake, this whitepaper doesn't seek to address all the points in the GDPR, and you should engage your own council when evaluating your requirements under the law.

Seeking Consent

Under the GDPR, subjects must give permission to have their data processed by a 'clear affirmative act'. This is an arrangement between the 'controller' who determines what is done with the information, and the 'subject' upon which the information is based. The legislation also recognises 'processors', such as StarRez, who act upon that data for the controlling institutions. Processors are also required to comply with the GDPR, but consent doesn't need to be sought by them, provided it has been given to the controller for that purpose.

Silence, pre-ticked boxes or inactivity are all given as examples that do not meet the requirements for consent. When subjects do give their consent, it must be for a specific, unambiguous purpose, upon which the subject has been informed, and must cover each of the purposes for which the data will be used. Consent must be able to be withdrawn without detriment for it to be considered legitimate.

Writing a clause into a contract, such as for accommodation, is sufficient to satisfy the requirement for consent, but only for the data required to perform that contract. Any pre-written declaration of consent needs to be in clear and plain language. If you intend to use the data for other purposes, such as alumni and marketing, then subject must provide consent for those activities, and have a genuine choice in whether their data is used for that purpose.

Minors have specific protections under the legislation, and their parent or guardians must also give their consent if they are under 16. In particular the GDPR calls out any instance where that data will be used for offering services directly to the minor, creating user profiles, or marketing as all requiring parental consent. One area where parental consent is not required is in the context of preventative or counselling services offered directly to the minor.

The GDPR also calls out automatic decisions that are based on information given, such as auto-allocation, or roommate matching. If your institution is using these functions, you will need to make it clear to the end user what details are used during the matching process at the time when they enter their data and provide consent to use it for the purpose of being assigned a room. Subjects have the right to obtain human intervention in any such system to express their point of view and obtain an explanation of the decision reached, and potentially challenge it.

Importantly, the GDPR requires that a child under the age of 16 should not be subject to automated decision making based on their personal data, such as auto-allocation.

Further information:

- GDPR Recitals 32, 38, 42, 43, 71
- GDPR Article 7
- EU Opinion Article 15/2011 on Consent

Breach Notification

If StarRez becomes aware of a breach, we will report it to our affected customers within 24 hours. If your institution becomes aware of a breach, you are required to provide notice to the appropriate supervisory authority within 72 hours. This is not required in instances where the institution can demonstrate that the breach is unlikely to result in a high risk to the subjects affected (for example, if the information was encrypted).

If there is a high risk to the data subjects affected, then they must also be informed 'as soon as reasonably feasible'. This communication must include:

- The nature of the personal data affected
- Recommendations for mitigating the potential effects of the data lost

There are a range of penalties in the legislation for delays in notification, including the supervisory authority directly notifying the subjects, and increased fines. One allowable instance for delay is if early disclosure would unnecessarily hamper an investigation by law enforcement.

Further information:

- GDPR Recitals 85, 86, 87, 88
- GDPR Articles 33, 34
- National Data Protection Authorities

Right to Access

The new legislation creates an obligation on the data controller to provide any data it has on the subject in an easily understood format. This includes the requirement to provide the data in a

common, portable data format (such as .PDF), as well as stating that if the data is hard to understand in its raw format, it should be made easier to understand, such as by providing visualizations.

The GDPR states that the requests should be responded to 'without undue delay', and gives a time limit of one month at the latest. There are some situations in which a data controller is not required to provide access to this data:

- The subject already has access to the data
- Recording the data is required by law
- It would involve disproportionate effort

Where possible, the data controller is required to provide remote access to a secure system which provides the subject with access to their data directly, such as PortalX. If any of the data kept on the subject is incorrect, the data controller must correct it when requested. Additionally, if it is technically possible to transfer the information directly to another data controller (a competing institution), the data controller must do so when requested.

Further information:

- GDPR Recitals 59, 62, 63, 68
- GDPR Articles 13, 15, 20

Right to be Forgotten

This is officially referred to as the *right to erasure* under the legislation, and gives subjects the right to have their data removed from the controller's system. If the subject was a child when the data was originally gathered, and their legal guardians gave consent instead, once the subject is no longer a child, they may then request the information erased. In the event that the controller has made the subject's information public, they are obliged to contact other controllers which are processing the data (such as search engines) and pass on the request for erasure. You can see examples of these removal mechanisms here:

- Google EU Privacy Removal
- Bing EU Privacy Request

There are legitimate circumstances in which a data controller does not have to erase the data they hold. These include:

- Where data is required to be kept for legal reasons (e.g. Finance, HR) – in these cases you would need to erase all data except that which is legally required
- Expressing the right of freedom of expression – for example, someone's name is publically used on your site in a reasonable manner, they are not automatically granted the right to have you remove it
- Where it is in the public interest, such as for law enforcement
- Scientific research, statistics, and other areas. These are not likely to apply to commercial operations

There has been some conjecture around whether the right to erasure also includes removing an individual from backup records. The EU has not provided definitive advice on this, or whether retaining a subject's information as part of a backup constitutes 'processing'. Most backups feature encryption and row-based integrity hashes, making removing individual records well outside the scope of being commercially reasonable. Backups are required to meet the data protection and integrity requirements in the GDPR, so erasing all of them due to a single record would not satisfy the legislation either. Until the EU provides a ruling, a potential solution would be to put in place an organisation measure to remove any affected records in the event that backup are restored.

Further information:

- GDPR Recitals 65, 66
- GDPR Articles 16, 17

Privacy by Design

The concept of privacy by design is intended to ensure that privacy-protecting practices are engineered into all of an institution's processes, rather than being considered as an afterthought. This requires reviewing all appropriate processes and implementing principals such as the following:

- Only keeping data necessary to perform the services offered
- Limiting access to that data to the minimum set of people who need to see it
- Making information behind how that data is used (auto allocation, roommate matching, etc.) transparent
- Allowing the subject to monitor the data processing
- Ensuring the data is securely stored, protected, and erased once no longer needed
- Performing data protection impact assessments

As part of implementing privacy by design, roles and responsibilities must be formally recorded, along with internal policies which demonstrate compliance. The legislation does not endorse a specific standard for doing this, however it identifies industry standards, such as ISO 27000, COBIT, or SSAE-16 as an appropriate method of demonstrating compliance. Whichever standard your institution uses, the privacy by design related processes need to be merged in with it in order to demonstrate compliance.

To ensure compliance with the GDPR, it is also required that an institution only employ data processors (such as StarRez) that have sufficient expertise, resources and commitment to implement the technical and organisational measures to meet the legislation. This adherence should be governed by a contract, such as a Data Processing Agreement. StarRez will be developing and providing a Data Processing Agreement by January 2018.

Further information:

- GDPR Recitals 78, 81
- GDPR Article 25

Data Protection Officers (DPOs)

Most institutions that process data are required to appoint a Data Protection Officer (DPO). This is mandatory for any institution whose *'core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale'*, which applies to any housing operation. Data Protection Officers must meet a series of criteria:

- They must be formally appointed by a written mandate;
    - They must report to the highest level of management
    - They may not be instructed how they are to perform their duties, and may not be dismissed or penalized for performing those tasks
    - This person will be compelled to provide evidence in the event of non-compliance by the institution
- They must have an understanding of the data processing that the institution performs
- They must have expertise in EU Privacy Law and implementing Data Privacy Programs

Notably, it is not required that a DPO is full time, and they may be employed on a consultancy basis. This creates an opportunity for multiple institutions to share a DPO, which is a service likely to be offered by legal firms and other consultants. If your institution adopts this approach you need to ensure that any 3rd party engaged has a solid understanding of the services you provide; a generic approach will not meet GDPR requirements. A trained DPO can provide further guidance on the requirements of the legislation, such as data protection impact assessments and the records that must be kept under law.

Further information:

- GDPR Recital 80
- GDPR Articles 27, 37, 38
- EU Guidelines on Data Protection Officers

Concluding Notes

The GDPR is an extensive piece of legislation which will change how most institutions conduct business. Institutions (who are data controllers and processors), and supporting companies like StarRez (a data processor) both have non-transferable obligations to address.

As part of GDPR regulations, it is only permissible to transfer data to other countries or institutions with the same level of privacy protection as the EU/UK. In the case of StarCare support, this will be met by certification against the EU-US and Swiss-US Privacy Shield Framework. This guarantees appropriate levels of protection for private data, and addresses the legal implications from the transfer of data.

If you have further questions regarding the GDPR legislation, and how StarRez can help you become compliant, please contact Client Relations, or dpo AT starrez.com.