

The image features a background of a woman in a business suit, seen from the side, looking towards the left. The background is divided into three colored triangular sections: blue at the top left, yellow at the top right, and green at the bottom. The HRACUITY logo is positioned in the top left corner, with 'HR' in white and 'ACUITY' in green.

HRACUITY®

**HOW
HR ACUITY
HAS PREPARED FOR**

**General
Data
Protection
Regulation**

The background of the slide features a photograph of two women in a professional setting. One woman, with blonde curly hair, is seated and looking at a laptop. The other woman, with dark hair and glasses, is standing and pointing at the screen. The image is overlaid with a semi-transparent blue geometric pattern consisting of interconnected triangles. The text is positioned in the lower-left quadrant of the image.

SECTION 1

A SHORT GUIDE TO GDPR

Section 1: A Short Guide to GDPR

WHAT IS GDPR?

The EU General Data Protection Regulation (GDPR) is a new regulation that replaces the 1995 EU Data Protection Directive. It sets new standards for the collection, use, processing and transfer of personal data of European Union citizens. Significant and wide-reaching, the new law brings a 21st Century approach and fundamental rights for European Union citizens living in the digital world.

WHEN IS THE REGULATION EFFECTIVE?

May 25th 2018. Previous national data protection laws in EU countries are replaced by GDPR.

WHAT IS THE REACH OF GDPR?

It applies to all European Union member states and also any country or entity that transfers the personal data of EU citizens outside of the European Union.

WHAT IS THE OBJECTIVE OF GDPR?

GDPR provides a single set of rules for data protection across Europe.

Firstly, GDPR seeks to expand the rights of individuals over how organizations use their personal data and to bring data protection law in line with how people's data is being used. The internet and the cloud have allowed organizations to develop new methods to use (and abuse) personal data since the 1995 Directive. GDPR aims to control this by placing new obligations on organizations to be more accountable for data protection. The second driver is the EU's desire to making data protection law identical throughout member states to give organizations more clarity over how they can behave.

HOW DOES GDPR RELATE TO PRIVACY SHIELD?

The EU:US Privacy Shield Framework allows organizations to transfer data to the US where this Framework is adopted. US companies, like any companies in the EU, must still comply with all the requirements of GDPR when collecting personal data.

Section 1: A Short Guide to GDPR

HOW DOES GDPR RELATE TO BREXIT?

The UK will still be part of the EU when GDPR comes into effect and, as such, GDPR will apply. Once the UK has left the European Union, the UK Data Protection Act 2018 has ensured the UK still has to comply with the requirements of GDPR.

WHAT CONSTITUTES PERSONAL DATA?

GDPR expands the definition of personal data. What constitutes 'personal data' is much broader and it specifically covers 'online identifiers'. Personal data is all information that can be linked to an identifiable individual, either directly or indirectly. This means that even data with no direct identifiers (such as name or address) could be considered personal data.

WHAT IS THE DIFFERENCE BETWEEN A DATA CONTROLLER AND A DATA PROCESSOR?

GDPR places obligations on a data controller and a data processor.

A **data controller** is an entity that determines the purposes, conditions and means of the processing of personal data.

A **data processor** is an entity that processes personal data on behalf of the controller under instruction.

A woman with curly hair is looking at a tablet. The image is overlaid with a semi-transparent geometric pattern of triangles. The text is positioned on the left side of the image.

SECTION 2

GDPR AT HR ACUITY

Compliance for the collection, usage, processing and transfer of personal data in relation to the HR Acuity Employee Relations Technology Solution

Section 2: GDPR at HR Acuity

HOW HAS HR ACUITY PREPARED FOR GDPR?

- We have invested in legal advice for reliable interpretation of the legislation for our businesses.
- We have reviewed, documented and continue to review the data we hold and our data process.
- We have updated our privacy policies.
- We have appointed Data Protection Officers (DPOs) in the US and EU.
- We have addressed our ability to enable our clients to provide personal data information upon request and comply with the right to be forgotten and data portability.
- We have adopted a data protection by design and default process within our organization.
- We continually identify and monitor all information risks and risks to the rights and freedoms of individuals.
- We have prepared and implemented a data breach notification process.
- We continue to ensure appropriate technical measures to secure our information and have a robust training schedule in place for all our staff.

Section 2: GDPR at HR Acuity

WHO IS THE DATA CONTROLLER AND DATA PROCESSOR FOR HR ACUITY?

HR Acuity Employee Relations Technology Solution gains access to employee personal data through our clients. Therefore, our clients are the Data Controllers and HR Acuity is the Data Processor.

WHAT TYPE OF PERSONAL INFORMATION DOES HR ACUITY PROCESS?

Within HR Acuity, each organization determines what type of information to be provided to HR Acuity and stored within our solution. The following employee information are examples of information that may be stored within HR Acuity and could be considered personal data:

IDENTIFIABLE INFORMATION SUCH AS:

- Name
- Audio and video recordings
- Work email address
- Personal email address

PROFILE/SENSITIVE/SPECIAL CATEGORY INFORMATION SUCH AS:

- Job title
- Performance or disciplinary records
- Race or ethnic origin
- Gender
- Age or birthdate
- Trade union membership

The exact data to be processed will be documented and contained within the instructions to HR Acuity to process with the Controller.

ADDRESSING THE RIGHTS OF INDIVIDUALS

Under GDPR, Controllers are responsible for responding to requests for exercise of rights by data subjects including the right to be forgotten, right of access and right to rectification. Our system has been developed to assist Controllers in responding to these requests, and can be managed through our administrative features on an as-needed basis.

Section 2: GDPR at HR Acuity

ADDRESSING DATA PROTECTION BY DESIGN & DEFAULT

Our solution and any future enhancements are designed and developed in ways that meet the GDPR requirements. This will include a review of the data flows, data items and management of any identified risks..

When HR Acuity uses with any third-party services that may impact our client data, they need to prove GDPR conformity in order to remain an HR Acuity partner and will be instructed under contract as per GDPR requirements.

HANDLING BREACH NOTIFICATIONS

Under GDPR, our process is in place so that:

- The Processor shall notify the Controller as soon as possible after becoming aware of any personal data breach.
- Any potential breaches are reported to the Controller within 24 hours, ensuring that the Controller has the ability to report to the identified national Data Protection Authority within 72 hours.
- As part our compliance monitoring, we audit the response times to Controllers for any identified breaches.

Please note:

This document does not supply legal or procedural advice for any company's GDPR compliance. Further information regarding GDPR compliance when working with HR Acuity, please contact us at gdpr@hracuity.com.