SOLA | Consulting

SG ST SC

The GDPR In Recruitment

Julian Jordan, Lead GDPR Consultant - SOLA Group

www.solagroup.com

SOLA Consulting

SG ST SC

Introductions:

Julian Jordan:

- 20 years IT Security Consultancy
- Sectors: Retail, Banking, Professional Services, Security Services
- Roles: Security Solutioning, Infrastructure, Regulatory Change, Business Transition and Transformation, Outsourcing Programmes, and Process Re-Engineering
- Regulatory Programmes driven by ISO27001 & ISO9001, FCA, BOE
- Lead GDPR Consultant: SOLA, Barclays Plc., Direct Line Group, Jigsaw

Tania Bowers:

- Solicitor in professional staffing sector since 1999
- Head of Legal and Compliance & Group Legal Director
- Director of Legal Consultancy
- General Counsel of APSCo

The GDPR Overview:

"The GDPR" is the new General Data Protection Regulation, superseding the UK Data Protection Act 1998. It is a legal obligation for companies to protect their customer and their employee Personal and Personal Sensitive data.

The GDPR applies to all companies that trade in and with Europe, those who have European customers, European offices, or European employees.

A UK Bill is due for release in September 2017, making the GDPR part of UK law post Brexit. Brexit will NOT affect this legal stance, the UK and Europe will both have to abide by the new laws from May 2018.

It is a pragmatic and necessary regulation, to put control into the ever changing cyber landscape that facilitates our business and personal lives.

To become compliant with the GDPR, a transitional period of change is to be expected.

Data

At the core of the GDPR, Data is one of the four major quadrants. Fundamentally, the regulation is concerned with customer and employee Personal and Sensitive Personal Data.

According to the European Commission “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.”

Explicitly, the GDPR is regulating the way that companies Receive, Process, Store, Manage, Handle, Consolidate, Retain, Share, and Protect customer Data.

Failing to protect this data, can and will result in harsh penalties

How does this affect Recruitment?

Personal Data is at the core of the GDPR. In that statement from the European Commission, almost every piece of Personal Data listed is used by recruiters. Let's break down the average CV:

1. Name
2. DOB
3. Telephone number
4. Email Address
5. LinkedIn Address
6. Personal Summary
7. Employment History
8. Qualifications
9. Education
10. Personal Interests

It's all Personal Data. It all has to be protected

How does this affect HR?

Human resources are an even higher risk. They not only handle CVs, but they manage employees Sensitive Personal Data. Let's break that down:

1. NI number
2. Salary, Pension and Benefits
3. Ethnicity
4. Healthcare and Sickness Leave
5. Religious Requests
6. Legal Disputes
7. Disciplinary Actions
8. Internal Employment History
9. Internal Qualifications

Most of this is Sensitive Personal Data and all needs to be protected

Where are the dangers?

The dangers for industries that rely heavily on Personal Data are higher than those that do not. *Some* of the key areas of concern for the Recruitment industry are:

1. CV management
2. Candidate Compliance
3. Security Vetting
4. Lawful Processing: Explicit Consent
5. Sharing Personal Data
6. Storing Personal Data
7. Cloud Services
8. CRM systems
9. ATS Systems
10. Candidate Offers
11. Contractual Obligations
12. Marketing

Getting it wrong here will result in penalties

The Penalties

Quite Simply: Huge

- 4% of your last annual turnover (GDP), or Euros 20,000,000 (whichever is greater)

How?

- By losing just 3 items of all of your customers Personal Data

Who?

- Financial data collectors (i.e. Banks)
- Companies for whom the ICO receives complaints
- Companies with historical data breaches
- Marketers
- Sensitive data collectors (i.e. Recruitment)
- Heavy data resellers (i.e. Social Media firms)
- Tax evaders
- Random selection

The GDPR is a bold statement – which demands bold enforcement

The Benefits

The GDPR has some very clear benefits:

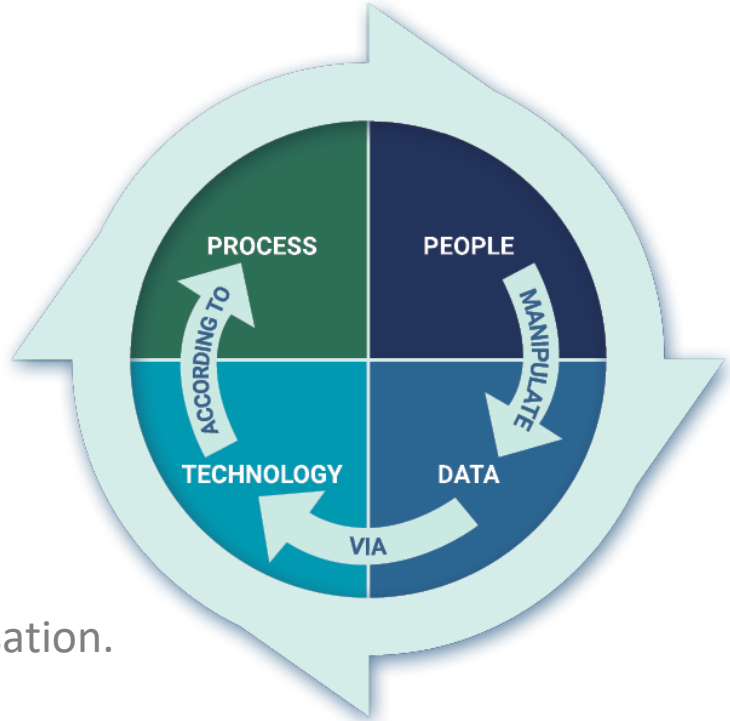
- The GDPR protects your customers' interests
- It protects your employees' interests
- It protects your essential assets: your IP and Data
- It builds customer and consumer confidence
- It secures your organisation
- It reduces long term operational costs
- It gives your business a competitive edge
- It increases staff efficiency through security awareness
- It is morally and politically correct

Becoming compliant with the GDPR is more than just a tick-box regulation. It can be viewed as a "CSIP" - a Continual Service Improvement Programme (an ITIL Service Management process)

If you were to build a new company tomorrow, the GDPR would be your blueprint

The Four Quadrants of the GDPR

Personal Data is manipulated through the four quadrants of GDPR:



These four quadrants represent your entire organisation.

Where to Start?

This is a Data Regulation. There is an obvious path in terms of priority, and that is an Audit or Assessment of where you and your data are today. Some start-up questions:

A. What Personal and Sensitive Personal Information do you hold?

B. Where is it?

C. Is it fully protected at rest and in transit?

D. Who has access to it?

E. Why do you need it?

F. Who owns it?

G. Do you have consent to use it or another lawful ground for processing it?

H. Where are the policies and processes for it?

I. How long can you legally keep it?

J. Is it backed up?

K. Where are the risks of data loss?

L. Is it shared with 3rd Parties? Are they actively seeking GDPR compliance?

M. Who are the Controllers and the Processors?

N. Digest the ICOs website

Mandatory Requirements

The next logical step is to look at the Mandatory Requirements, from 39 of the 99 Articles. Some of these include:

1. Perform an Assessment on your current operating state (Approx. 120 man hours)
2. Appoint a Data Protection Officer OR delegate responsibilities
3. Update Company Policies and Processes to reflect the regulation
4. NEW: Lawful Processing and Consent – at all customer data entry points
5. NEW: Data Portability and Data Deletion mechanisms
6. NEW: Data Breach mechanisms
7. NEW: Privacy By Design
8. Technical security for the data
9. Full process suite for handling Personal and Sensitive Personal Information
10. Laying a clear audit trail from Customer Consent to Data Usage

Quick Wins

Strategic Quick Wins:

a. Assign a GDPR Compliance Owner
b. Initiate an Audit on your People, Process, Data and Technology
c. Set up an organisation-wide GDPR Programme
d. Lay down an audit trail
e. Engage legal support

Tactical Quick Wins:

a. Ratify your use of Personal Data: Do you need DOB, or just YOB?
b. Store your candidate Data in one place
c. Agree and implement a data retention period
d. Ask IT to ring-fence your team, and protect said Data
e. Implement a “clean-desk” policy
f. Digitise all paper records, put them within the ring fence
g. Get someone to OWN this

Summary: Defensible Position

- On May 25th 2018, you must be in a “Defensible Position”
- Imagine defending your actions in a courtroom situation
- All GDPR efforts must be auditable
- Key considerations:
  - Change is mandatory
  - 100% Compliance is NOT achievable
  - Inaction will be punished – keep a trail of efforts
  - Fines for non-compliance & criminal offences
  - Reputational damage
  - Positive actions will be rewarded
  - Process changes MUST be implemented
  - The ICO may randomly pick organisations
  - The ICO will outsource to auditors
  - Unresolved Issues must have remediation plans
  - Infrastructure must be fit for purpose
  - Computers don’t make breaches, people do

SOLA Consulting

SG ST SC

Contact Details:

M: 07968 295 282

Email: julian.jordan@solagroup.com

My preferred contact channels:
Face to face at SOLA's Stand (45) today
Direct phone call or email

Tania Bowers

t.bowers@foxgrovelegal.com