GDPR vs Data Protection Act

R3Location
Reliability Reputation Relationships

General Data Protection Regulation replaces Data Protection Act on 25 May 2018.

Much has been made of the introduction of this new EU Regulation over the last few months. Whilst it is true that GDPR marks a significant development in the field of EU Data Protection, the practical application of the changes required for small UK businesses engaged in Destination Services or related field will not be that material if you are already compliant with the current Data Protection Act.

If, like R3Location, you are wondering what the **key differences** are between DPA and GDPR on the current running of your business in the context of destination service provision in the UK, this factsheet should be useful.

We hope to **alleviate some of the fear factor** surrounding this topic and to **provide greater clarity** on their practical effect, if any, if you are running an small (under GDPR criteria) UK-based business such as ours.

Key Steps towards compliance

1 Audit

Understand the current flow of personal data in your business, and why/how you process data

2 Checklist

What actions are likely to come out of your audit in order to be compliant with GDPR over and above DPA compliance

3 Terminology

What are some of the new terms to be familiar with under GDPR

4 Differences

Individual rights re: personal data remain broadly unchanged – so what are the key differences under GDPR?

1- Audit: know your data flow

Starting point: Understand the current flow of personal data in your business, and why/how you process data

Collecting

- Do you act as a data controller or processor?
- Who do you collect data from? What kind of data?
- Has consent already been acquired by your client?

Storing data

- Where do you store the data? Is it accurate?
- Do you use Cloud solutions or own server? Is it secure?
- Do you store it in more than one system? Can you consolidate?

Using/altering

- How do you use/change the data?
- Is it to provide relocation services? Maintain employee records? Marketing?
- Do you share it with your own sub-contractors?

Deleting data

- Is this data necessary to comply with your contractual obligations?
- Do you really need it?
- Do you have a data retention policy? Do you actually action it on ongoing basis?

2- Checklist: what do you need to change?

Consider: what are you likely going to have to put in place as a result of GDPR over and above DPA?

- ❑ Update Data Privacy policy to include lawful basis
- ❑ Is it easily accessible?
- ❑ Is your IT system secure?
- ❑ Have you checked with your IT providers?
- ❑ Are your servers safe?
- ❑ Have you amended terms and conditions with your suppliers?
- ❑ Have your clients sent you updated terms?
- ❑ Have you updated your Data Protection Policy?
- ❑ Do you have an opt-out on marketing material (assuming B2B)?

3- Terminology: so what's new?

Know your terms: In the main, as a DSP or related business, you are likely to be a processor as far as assignees' personal data is concerned. You still have some obligations, but not as onerous as a controller's.

Data Controller

A controller determines the purposes and means of processing personal data. As a DSP or related business, you are **likely to only be a controller** in the context of your employees' personal data and marketing data.

Data Processor

A processor is responsible for processing personal data on behalf of a controller (in most cases – your corporate client). You are required to **maintain records** of personal data and **processing activities**. You will have legal liability if you are responsible for a breach.

Lawful basis

From 8 principles to 6. These focus on the intent with which data is accessed and used being lawful, fair and transparent - and for specified explicit and legitimate purposes, and relevant and limited to what's necessary. **Know which applies to you.**

4- Differences: which are the key changes?

EU Regulation: Introduces some additional obligations across key areas – make sure you know what they are

			So what does this mean?
Definition of Personal Data	DPA	Personal data and sensitive personal data	Same as before – just catches additional type of data. Make sure you can identify which is relevant to you
	GDPR	Now includes online identifiers, location data and genetic data	
Accountability	DPA	Limited	Undertake Data Audit (see above), implement appropriate measures, document policy
	GDPR	Fully explicit that it is your responsibility to comply with GDPR principles	
Data Consent	DPA	Freely given, specific and informed	Likely only to affect data controllers – for DSPs this includes employees and marketing data (not B2B)
	GDPR	Clear affirmation action with ability to be withdrawn at a later date	
Responsibilities	DPA	Data controllers only	Make sure you undertake Audit as suggested in 1, and undertake appropriate changes
	GDPR	Rests with both controller and processor	
Breach notification	DPA	Not mandatory for most organisations	Note that proportionality comes into play here and you can assess if notification is required case by case
	GDPR	Mandatory and with 72 hours	
Data Governance	DPA	No need for a business to have dedicated Data Protection Officer	Unlikely to affect many DSPs and related businesses but some will opt for voluntary DPO governance
	GDPR	DPO mandatory subject to certain criteria (e.g. more than 250 employees)	
Fines	DPA	Maximum fine is £500,000	Unlikely to affect small businesses – such fines will be proportionate and for major infringements – not minor ones
	GDPR	Maximum fine is 4% of annual turnover or Euro 20m whichever is greater	

This factsheet is not a comprehensive guide to GDPR. It has excluded several other changes to the Regulation that may well apply to your individual businesses. We have focused here on the more material aspects and the ones that are more likely to be relevant for UK based DSPs or related businesses within the relocation industry.