

---

# What B2B Companies Should Know About GDPR

Tuesday 10<sup>th</sup> July

---

Nicola Howell, Senior Compliance & Privacy Attorney at  
Dun & Bradstreet



# Topics

---

Introduction

---

Does the GDPR Apply to my Business?

---

What is Personal Data in a B2B Context?

---

GDPR: An Evolution, Not A Revolution

---

I'm a "Controller" – HELP!

---

# Introduction



What to consider if any of your customers are unincorporated businesses (such as sole traders or partnerships).



Legal considerations if your business processes data relating to the personnel of your customers and what this means about further uses of the data.



GDPR implications if your customer list is unlawfully hacked or stolen.



GDPR implications of transferring data outside the EU.



Marketing to your customer list under GDPR.

# Does the GDPR apply to my business?

“I’m a B2B company and General Data Protection Regulation applies to “personal data” - therefore GDPR does not apply to my company...”

**WRONG!**

“Personal data” is any information relating to an identified (or identifiable) natural person ('data subject').

There are no exemptions or differentiations between personal and business data.

# What is Personal Data in a B2B Context?

Where are we with processing it?

1. Employees

2. Customer Contact Data  
(including prospect and  
historic)

3. Vendor Contact Data

# Employee Personal Data



All B2B businesses are processing this.

Not just employees:

- Job Applicants
- Ex Employees

Often the most problematic personal data any business processes:

Illness? Religion? Sexuality? Criminal convictions? – these are all sensitive under EU law.

Bank account details? Remuneration package – these are high risk.

# Customer Personal Data



The most important personal data for commercial reasons!

- Contact Information
- Payment Information
- Payment History
- Compliance Checks? - Including information on Directors, Shareholders, Trustees, Sole Traders, Partnerships

# Vendor Personal Data



Back office data:

- Contact Information
- Payment Information
- Compliance Checks? - Including information on Directors, Shareholders, Trustees, Sole Traders, Partnerships



# How Do We Manage This Personal Data?

In accordance with GDPR!

2 roles under GDPR:

- Controller
- Processor

Processor acts on behalf of the Controller – a service provider, an outsourcer

**Good news** – B2B businesses are unlikely to be holding personal data as a Processor

# An Evolution, Not a Revolution

dun&bradstreet

FOR PUBLIC USE

# GDPR: An Evolution, Not a Revolution



GDPR wasn't started with a blank canvas



The principles, grounds of processing and many definitions have remained the same as current/previous data protection laws – you may be more compliant than you realise.



There are many misunderstandings and myths...

# ICO Guidance

The ICO will not be bringing any prosecutions on 26<sup>th</sup> May

Liz Denham made a speech at the ICO conference April 2018

Continuous improvement

“

*I hope by now you know that enforcement is a last resort. I have no intention of changing the ICO's proportionate and pragmatic approach after 25<sup>th</sup> May. Hefty fines will be reserved for those organisations that **persistently, deliberately or negligently flout the law.***

LIZ DENHAM

“

*Those organisations that self-report, **engage with us to resolve issues** and **can demonstrate effective accountability** arrangements can expect this to be a factor when we consider any regulatory action.”*

LIZ DENHAM

“

*It's important that we all understand there is no deadline. **25 May is not the end. It is the beginning...** We are days away from the first day of a new era for data protection.”*

LIZ DENHAM

I'm a "Controller"  
– HELP!

dun&bradstreet

FOR PUBLIC USE

# I'm a Controller – HELP!



What does this mean?...

Controllers “determine the purposes and means of the processing of personal data”

They are literally **in control** of the data.

# Where to Start?



1. Get an overview of what personal data.
2. Assess whether it is all needed – if not discard and stop receiving.
3. Assess how long each type of data needs to be retained for – discard?

# Assess What “Ground” You Are Processing Data Under



## Consent?

*There are 6 grounds in the GDPR – consent is problematic:*

- *Explicit*
- *Can be withdrawn*



## Article 6...

- *Necessary for the performance of a contract to which the data subject is party*
- *Necessary for compliance with a legal obligation to which the controller is subject*
- *Necessary for the purposes of the “legitimate interests” pursued by the controller*



# Assess Your Data Subject Rights



You can only do this once you know the legal ground for processing.

Does your business need a Data Protection Officer?

Data subject rights will mostly apply in HR context:

- Right to Rectify
- Right to Information:
  - Subject Access Requests
  - Privacy Notices



Visit our GDPR Hub at [www.dnb.co.uk/gdpr](http://www.dnb.co.uk/gdpr)