The new General Data Protection Regulation
What furniture companies need to do to be compliant!

Wednesday 15th November 2017 at Cranmore Park

Catherine Herries-Smith

THEMES
What are the key concepts?

1. Controller and Processor
2. Must process in accordance with principles
3. Must process in accordance with conditions
4. Specific rights for individuals
5. Enforcement by supervisory authorities

THEMES
What are the key definitions?

- Personal data

‘means any information relating to an identified or identifiable natural person (‘data subject’)’;

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.’

Eg: John.Smith@Toolsmiths.com

THEMES
What are the key definitions?

Special categories of personal data

Racial or ethnic origin	Political opinions	Religious or philosophical beliefs
Trade union membership	Genetic data (new)	Biometric data (new)
Health data	Sex life and sexual orientation	

THEMES
What are the key definitions?

Controller

‘means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing personal data;

Processor

‘means a natural or legal person, public authority, agency or any body which processes personal data on behalf of the controller’

THEMES
What are the new data protection principles?

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality

(Art. 5)

6 instead of 8

THEMES
Data protection principles

1. Lawfulness, fairness and transparency

‘Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject’.

THEMES
Data Protection principles

2. Purpose limitation

‘Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way compatible with those purposes; further processing of personal data for archiving purpose in the public interest, or scientific and historical research purposes or statistical purposes shall, in accordance with Article 83(1) not be considered incompatible with the initial purposes of lawfulness, fairness and transparency’

THEMES
Data Protection principles

3. Data Minimisation

‘Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed’.

THEMES
Data Protection principles

4. Accuracy

‘Personal data must be accurate and, where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, erased without delay’

THEMES
Data Protection principles

5. Storage Limitation

‘Personal data must be kept in a form which permits identification of data subjects for no longer that is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 83(1) subject to implementation of the appropriate technical and organisation measures required by the Regulation in order to safeguard the rights and freedoms of the data subject’.

THEMES
Data Protection principles

6. Integrity and confidentiality

‘Personal data must be processed in a way that ensures appropriate safety of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures’.

THEMES
significant areas of change under GDPR

1. Extraterritorial reach
2. New processing conditions
3. New individual rights:
   I. right to be forgotten
   II. right to data portability
   III. right to restrict
4. Data protection officer role
5. Data processors have liability
6. Increase in sanctions

1. ORGANISATION COMPLIANCE Introduction

What does your organisation need to put in place to ensure it is ready for the GDPR?

a. Data protection by design and default (eg at outset consider data minimisation and pseudonymisation)
b. Data Protection Officer (public bodies, core activities require large scale monitoring of individuals or core activities consist of large scale processing of special categories of data

1. Organisation Compliance

c. Record keeping provisions

Potential exemption

Record keeping obligations generally won't apply where less than 250 employees

Exemption will not apply if:

1. Risk to rights/freedoms of individuals; or
2. Processing is not occasional; or
3. Processing includes special categories of data

Organisation Compliance
Records keeping

Controllers and processors shall maintain a record of personal data processing activities which include:

1. Name and contact details of the Controllers and DPO
2. The purpose and categories of processing (see following slide)
3. Description of security measures in place
4. Recipient countries and safeguards in place (if outside EU)

Organisation compliance
Record keeping

Additionally Controllers (but not Processors shall record):

5. Description of categories of personal data held
6. Categories of individuals whose data is held
7. Categories of recipients of data
8. The envisaged time limits for erasure

Record keeping
Information Asset Register

Categories of personal data	Purpose of processing	Categories of data subjects	Categories of recipients	Transfers out of EEA	Legal basis For processing *	Data retention period	Security measures

Organisation compliance

d. Security provisions

Controllers need to implement appropriate measures to ensure security is appropriate to the risk including (as appropriate):

a. Pseudonymisation and encryption
b. Ability to ensure confidentiality, integrity, availability and reliance
c. Ability to restore access
d. Process for regularly testing and evaluating security

ORGANISATIONAL COMPLIANCE
Security

- Controllers need to implement appropriate measures to ensure security is appropriate to the risk including (as appropriate):

a. Pseudonymisation and encryption
b. Ability to ensure confidentiality, integrity, availability and reliance
c. Ability to restore access
d. Process for regularly test and evaluating security

ORGANISATIONAL COMPLIANCE
Security

- Employee obligations: Controllers and Processors both need to ensure that those acting for them do not process other than on instructions of the Controller

- Mitigating breaches: Controllers need to take account of particular risks such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data which is being processed

ORGANISATIONAL COMPLIANCE
Impact Assessments

- If processing is likely to result in a high risk to individuals the Controller shall carry out impact assessments

Assessment is required if:

a. automated, systematic and extensive evaluation of personal aspects of the individuals which is the basis of decision concerning the person (e.g. profiling such as to evaluate to analyse individual's economic situation) or

b. Large scale processing of special categories of data; or

c. Systematic monitoring of a publicly accessible area on a large scale.

ORGANISATIONAL COMPLIANCE
Impact Assessments

- The impact assessment shall contain (at least):

a. Description of processing operation and purpose of processing

b. Assessment of

    necessity and proportionality of processing

    risks to rights and freedoms of individuals

a. Measures to address risks

b. Demonstration that GDPR and ICO's codes of conduct have been complied with and taken into account

OBTAINING DATA
Introduction

When collecting personal data from individuals, Controllers will need to consider:

a. What are the lawful grounds for processing?
b. What are the lawful grounds for processing special categories?
c. How to obtain valid consent for processing?
d. What information needs to be provided to the individual?

OBTAINING DATA
Grounds for processing

Controllers need to consider lawful grounds for processing which are:

1. Provided **consent**
2. Necessary for

a) the performance of a **contract** with individual

b) compliance with the Controller's **legal obligations**

c) protection of individual's **vital interests**

d) performing task in **public interest**

e) **legitimate interests** pursued by Controller

OBTAINING DATA
Grounds for processing special categories

Processing special categories of personal data is prohibited unless:

1. **Explicit consent** provided by individual
2. Individual made the data **public**
3. Processing is carried out in course of **legitimate activities**:

a) with appropriate **safeguards** in place;

b) by political, philosophical, religious or trade union not-for-profit body; and

c) the processing relates solely to members, former members or those with regular contact in connection with purposes

OBTAINING DATA
Grounds for processing special categories

4. The processing is **necessary**

a) For **employment** law obligations
b) To protect individuals **vital interests** (if unable to consent)
c) To establish, exercise or defend a **legal claim**
d) For **substantial public interest** on legal basis
e) For **preventative or occupational medicine**, assessment of **working capacity** of employees, medical diagnosis, provision of health or social care or management of health or social care systems or pursuant to contract with health professional
f) Reasons of **public interest** in area of **public health**
g) Archiving purposes in **public interest**, or **scientific** or **historical research** purposes or **statistical** purposes

OBTAINING DATA
Consent

Consent to process personal data must be:

i. Freely given
ii. Specific
iii. Informed
iv. Unambiguous indication
v. Clear affirmation

OBTAINING DATA
Consent: Children

- Children of 16 or over can potentially provide valid consent to processing their personal data
- UK can reduce this age but no lower than 13
- If below 16 (13) processing only lawful where consent given by the holder of parental consent
- Controller must make reasonable efforts to verify that consent is given by holder of parental responsibility

OBTAINING DATA
Providing information

Controllers **must** provide the following information to individuals when their personal data is collected:

i. Identity and contact details of Controller
ii. Contact details of DPO
iii. Purposes of the processing
iv. Legal basis for the processing
v. Recipients of the personal data
vi. If intend to transfer data outside the EU, details of adequacy decision and safeguards in place

OBTAINING DATA
Providing information

Controllers **should** provide the following information to individuals when their personal data is collected (if necessary):

i. The **period** for which the data will be stored
ii. Individual's **rights**
iii. The right to **withdraw consent**
iv. Right to lodge **complaint** with the ICO
v. Any **statutory** or **contractual** requirement to process
vi. Where data is required to enter into a **contract**
vii. Consequences of failing to provide the data
viii. If there is **automated** decision making

OBTAINING DATA
Providing information

Where data obtained through a third party

Still need to provide similar information to the individual

Also required to provide

i. Categories of personal data concerned; and
ii. The source of the data

Information must be provided either

a. Within a reasonable period from obtaining data; or
b. First contact with the individual; or
c. When data disclosed to a third party

OBTAINING DATA
Providing information

Change of purpose

- If processing the data for a new purpose, Controllers need to provide individuals with the same categories of information

Exemption

- The requirement to provide information doesn't apply if:

1. Individual already has the information; or
2. The data came from a third party and it is impossible or entails disproportionate effort, to inform the individuals

PROCESSING DATA
Using Processors

Controllers engaging Processors

Controllers need to ensure Processors guarantee they have in place appropriate technical and organisational measures

Processors engaging Processors

Processors can only engage Processors if the Controller has provided prior specific written authorisation

Controllers can provide general written authorisation to engage other Processors (but Processors need to inform Controllers in advance of any changes)

PROCESSING DATA
Processing agreements

Generally there must be a binding contract between the Controller and Processor which sets out:

I. The **subject matter** of the processing
II. The **duration** of the processing
III. The **nature** and **purpose** of the processing
IV. The **type** of personal data
V. Categories of **individuals**
VI. Obligations and rights of the Controller

PROCESSING DATA
Processing agreements

Contract must impose following obligations on the Processor

1. Data is only processed with Controller's **written instructions**
2. Employees are under **confidentiality** obligations
3. **Security** provisions are in place
4. Other Processors are only engaged if Controller provided **written consent** and the new Processor is bound by **same contractual terms**
5. Processor will **assist the Controller** with specified GDPR obligations
6. Processor will **delete** or **return** personal data to Controller
7. Processor will provide compliance information to Controller

INDIVIDUAL RIGHTS

- GDPR largely preserves existing rights of individuals in relation to:

- Subject access (Art.15)
- Rectify inaccurate data (Art.16)
- Object to processing (Art.19)
- Challenge automated decisions (Art.20)

INDIVIDUAL RIGHTS
GDPR

- GDPR creates significant new rights:

- Right to erasure (‘right to be forgotten’) (Art.17)
- Restrict processing (Art.17a)
- Right to data portability (Art.18)

INDIVIDUAL'S RIGHTS
Right of Subject Access

- Individuals have the right to obtain from the controller:

i. Purposes of the processing
ii. Categories of personal data concerned
iii. Recipients to whom data has been disclosed
iv. Where possible, envisaged period for which data will be stored, or, if not possible the criteria used to determine the period

INDIVIDUAL'S RIGHTS
Right of Subject Access

v. Exist of right to object and to request rectification, erasure and restriction of processing

vi. Right to lodge a complaint with ICO

vii. Where data not collected from individual, information about their source

viii. Existence of any automated decision making

INDIVIDUAL'S RIGHTS
Right of Subject Access

What do data controllers need to do?

- Upon receipt of a request, controllers shall provide a copy of the personal data
- If request made electronically, unless requested by the applicant, the information should be provided by electronic means

INDIVIDUALS' RIGHTS
Right of Subject Access

When can data be withheld?

Controllers can withhold data if disclosure would adversely affect the '*rights and freedoms of others*'

- Similar to existing third party data exemption
- Protects business as well as individuals; extends to commercially sensitive information, trade secrets etc

INDIVIDUALS' RIGHTS
Right to Rectification

Individuals have the right to:

1. Obtain from the controller rectification of data which is inaccurate; and
2. Having regard to the purposes for which data is processed, obtain completion of incomplete data, including by means of supplementary statement

INDIVIDUALS' RIGHTS
Right to Object

Provides a right to prevent certain processing

- GDPR reverses burden of proof:
- Controller must show compelling legitimate grounds to continue to process personal data, rather than individual having to show compelling grounds to stop processing

INDIVIDUALS' RIGHTS
Automated decisions

Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produce legal effects concerning him or her

The right will not apply where the decision is:

1. Necessary for entering into or performance of a contract between individual and controller; or
2. Is authorised by a Union or Members State law to which controller is subject; or
3. Is based on the individual's explicit consent

INDIVIDUALS' RIGHTS
Right to be forgotten

Individuals shall have the right to obtain from controller the erasure of personal data concerning him or her

- Subject to exemptions, upon request of individual controllers must:

1. Erase the personal data; and
2. If data has been made public, take reasonable steps to inform other controllers of the request for erasure

INDIVIDUALS' RIGHTS
Right to be forgotten

Controllers must comply in following circumstances:

1. Individual has objected to processing and there are no overriding grounds to justify the processing
2. Personal data is no longer needed for the purpose for which it was collected/processed
3. Individual has withdrawn consent and there are not other processing grounds

INDIVIDUALS' RIGHTS
Right to be forgotten

4. Data is being processed unlawfully
5. There is a legal obligation under Union or Member state law to erase personal data
6. Data was processed in connection with an online service offered to a child

INDIVIDUALS' RIGHTS
Right to be forgotten

Exemptions include where processing is:

1. Necessary for rights and freedoms of expression or information
2. For compliance with a legal obligation under Union or Member State law
3. In the public interest in the area of public health
4. For archiving or research
5. For legal claims

INDIVIDUALS' RIGHTS
Right to restrict processing

Individuals have the right to obtain from the controller the restriction of personal data in certain circumstances

- Provides individuals with the power to control or effectively 'quarantine' their data
- Allows individuals to limit the range of purposes
- Controllers will need to ensure that their systems are set up to indentify restricted data and limit access to it

INDIVIDUALS' RIGHTS
Right to Data Portability

Individuals have the right to receive personal data concerning him or her in a structured and commonly used format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided

- Data portability enhances subject access rights
- Right to request data is transferred from one data controller to another
- No right to charge a fee for this service

INDIVIDUALS' RIGHTS
Right to Data Portability

What type of information is caught?

- Only applies to personal data 'provided to' controller, eg content stored on a cloud service
- Unclear whether it includes other information such as purchase history

INDIVIDUALS' RIGHTS
Right to Data Portability

When does the right apply?

Only applies where controller is processing personal data in reliance on the processing conditions of:

- Consent; or
- Performance of contract

INDIVIDUALS' RIGHTS
Time scales for responding

When responding to a request from an individual asserting one of their rights controllers must:

- Provide information on action taken on a request **without undue delay** and, at the latest within **one month** of the receipt of the request
- Time may be extended for up to a further **two months when necessary**, taking into account the complexity of the request and the **number** of requests

INDIVIDUALS' RIGHTS
Charging

Can the data controller charge a fee for responding to individuals' rights?

No, fee can be charged, unless:

1. Applicant requests **further copies**, for which **reasonable fee based on administrative costs** may be charge; or
2. Request is **excessive or manifestly unfounded**, ro which a fee can be charged (or request refused)

DATA BREACHES
Definition – personal data breach

“a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”.

Article 4

DATA BREACHES
Notification to the ICO

Is the breach **unlikely** to result in a risk to the rights and freedoms of individuals

YES

-No need for Data Controller to report to the ICO

NO (eg reputational damage, identity fraud)

-Data Controller must notify the ICO

-Without undue delay

-Not later than 72 hours unless there is a “reasoned justification”

DATA BREACHES
Notification – minimum requirements

- In notifying the ICO, Controllers shall at least set out the following:
- A description of:

-The nature of the personal data including categories and approximate number of individuals and data records concerned;

-The likely consequences of the breach;

-The measures taken or proposed to be taken to address the breach and to mitigate possible adverse effects.

- The name and contact details of the Data Protection Officer

DATA BREACHES
Recording breaches

- Controllers must document **all** breaches (Art.33)
- Including:

-The facts surrounding the breach; and

-Its effect and the remedial action taken.

DATA BREACHES
Notification to individuals

- Is the breach likely to result in a **high risk** (narrower) to the rights and freedoms of individuals (Art.34)?

NO

-No need for the Controller to notify individuals

YES

-The Controller must notify individuals unless an exemption applies

(Not within 72 hours but without undue delay – need first to try to contain)

DATA BREACHES
Notification – minimum requirements

- Notification to individuals by Controllers must be:

❑ In clear and plain language; and

Made “without undue delay”

- And must include a description of:

❑ The nature of the personal data breach

❑ Details of the DPO

❑ The likely consequences of the breach;

❑ The measures taken or proposed to be taken to address and mitigate the breach; and

❑ Recommendations for the individual to mitigate potential adverse effects.

DATA BREACHES
Processor reporting requirements

- Must now report breaches to Controllers
- Without undue delay after becoming aware of breach
- No exemptions for reporting
- Guidelines to be issued

ENFORCEMENT
ICO investigative powers

- The ICO will have the following powers (Art.58)

- ❑To order Controllers and Processors to provide any information in requires for the performance of its tasks
- ❑To carry out Audits (investigations)
- ❑To conduct certification reviews
- ❑To notify Controllers and Processors of any alleged infringement of the GDPR
- ❑Access to personal data from Controllers and Processors
- ❑Access to any Controller or Processor premises, including access to data processing equipment

ENFORCEMENT
ICO corrective powers

- The ICO will have the following corrective powers (Art.58):
- To impose:
  - -A temporary or definitive limitation including a ban on processing
  - -An administrative fine
- To order
  - -Rectification, restriction or erasure of data
  - -A certification body to issue a certificate
  - -Compliance
  - -Communication of a personal data breach to a data subject
- To issue:
  - -Warnings
  - -reprimands

DATA BREACHES
Administrative fines

- “effective, proportionate and dissuasive” (Art.83)
- 2-tiered sanction regime:

➢Up to 20M euros (£17M) or 4% of the total worldwide annual turnover (whichever greater)

➢Up to 10M euros or 2% of the total worldwide annual turnover (whichever is higher).

REMEDIES
Administrative fines - infringements

	Of the basic principles for processing	
Non-compliance with an order imposed by supervisory authorities	Up to 20M euros	Of data subjects rights
	Of obligations regarding international transfers	

REMEDIES
Administrative Fines - infringements

In relation to appointment of Data Protection Officer	To obtain consent to the processing of personal data	To maintain written records of processing activities
	Up to 10M euros	
To implement technical and organisation measures	On joint controllers to agree their joint compliance obligations	To report breaches when required to do so

REMEDIES
Compensation

- Individuals can pursue either:
  - ❖ Controllers OR
  - ❖ Processors
- Includes pecuniary and non-pecuniary loss
- Controllers and Processors can claim back all or some of any award if not responsible for the breach, either in part or in full

PRACTICAL TIPS

- ❑ Raise awareness amongst staff, include the Board
- ❑ Benchmark compliance (assess extent to which already comply and level of change required)
- ❑ Appoint a Data Protection Officer if required
- ❑ Draft a timetable and strategy for compliance
- ❑ Establish a culture of monitoring, reviewing and assessing DP procesures (to minimise data processing and retention)
- ❑ Review/update policies, privacy notices (ensure transparent and easily understood)

PRACTICAL TIPS

- Create and implement (or update) a Privacy Policy to be provided to individuals.
- Set out how data will be
  - -Stored
  - -Processed
  - -Provided, if requested deleted
- Update current procedures for handling subject access requests

PRACTICAL STEPS

- Review/update:
  - -Data sharing agreements
  - -Data processing agreements
  - -Contracts with processors
  - -Supplier contracts etc

PRACTICAL TIPS
Requirements – record keeping

- **Controllers**
  - A record of processing activities
  - A personal breach register
- **Processors**
  - A record of all categories of processing activities carried out on behalf of Controller
- Ensure required minimum content is included
- Consider how records will be kept up to date

PRACTICAL TIPS
Requirements – data security breaches

- Create and implement (or update) a Data Breach Management Policy
- To ensure that there are procedures in place to:
  - Detect and investigate breaches
  - Rapidly and correctly report breaches
  - Contain the impact of breaches

PRACTICAL TIPS
Other considerations

- Children
- Create and implement new practices for
  - Confirming the age of individuals; and
  - Obtaining parental consent when processing the data of children
- Demonstrating consent
  - Review methods for seeking, obtaining and recording consent to ensure compliance
  - Review and amend forms.

DIRECT MARKETING

Data Protection Act

F**irst principle**: organisations must process personal data fairly and lawfully.

-If direct marketing involves personal data (ie name of person contacting) will usually need to tell individual who they are and that they plan to use details for direct marketing

-Organisations will need to tell people if plan to pass on their details, including selling or sharing for marketing and are likely to need their consent to do so.

Second principle – cannot use for other incompatible purposes

Fourth principle – accurate and up to date.

PRINCIPLES

Direct marketing covers the promotion of aims and ideals as well as the sale of products and services. This means that the rules will cover not only commercial organisations but also not-for-profit organisations (eg charities, political parties etc).

- In many cases organisations will need consent to send people marketing, or to pass their details on. Organisations will need to be able to demonstrate that consent was knowingly and freely given, clear and specific, and should keep clear records of consent. The ICO recommends that opt-in boxes are used.

Principles

- The rules on calls, texts and emails are stricter than those on mail marketing, and consent must be more specific. Organisations should not take a one-size-fits-all approach.
- Organisations can make live marketing calls to numbers not registered with the TPS, if it is fair to do so. But they must not call a number on the TPS without specific prior consent.
- Organisations must not make any automated pre-recorded marketing calls without specific prior consent.

Principles

- Organisations making marketing calls must allow their number (or an alternative contact number) to be displayed to the person receiving the call.
- Organisations must not send marketing texts or emails to individuals without their specific prior consent. There is a limited exception for previous customers, known as the soft opt-in.
- Organisations must stop sending marketing messages to any person who objects or opts out of receiving them.

Principles

- Organisations must carry out rigorous checks before relying on indirect consent (ie consent originally given to a third party). Indirect consent is highly unlikely to be valid for calls, texts or emails.
- Neither the DPA nor PECR ban the use of marketing lists, but organisations must take steps to ensure a list was compiled fairly and accurately reflects peoples' wishes. Bought in call lists should be screened against the TPS. It will be very difficult to use bought in lists for text, email or automated call campaigns as these require very specific consent (either where the specific organisation is named or it is within a precisely defined category of organisation).

Principles

- The ICO will consider using its enforcement powers including the power to issue a fine of up to £500,000 where an organisation persistently ignores individuals' objections to marketing or otherwise fails to comply with the law.