

DAVID
PHILLIPS/

GDPR Overview





- By the end of the session you will know all about:
 - GDPR – what it is
 - What it means for David Phillips
 - What we are doing to get ready
 - What it means for you
 - What you need to do
 - What happens next
 - Where to find more information



- What is GDPR?
- Why it is important
- When it is happening



[introvideo](#)

- General Data Protection Regulations
- New regulations covering personal data
 - any information relating to an individual person such as name, contact details, bank information etc
- It applies to soft copy information and hard copy information
- Mandatory for all businesses within each EU member state – including after Brexit

We can collect, store and use personal data *only* if it is:

- Obtained only for specific lawful purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not to be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Protected in appropriate ways
- Not be transferred outside of the European Economic Area
 - Unless that country or territory also ensures an adequate level of protection

- The GDPR provides greater rights for individuals:
 - To be informed
 - Access
 - Rectification
 - Erasure
 - Restrict processing
 - Data portability
 - To object
 - Rights in relation to automated decision making and profiling

When it is happening



What you need
to know about
GDPR

GDPR at David
Phillips

- What GDPR means for David Phillips and why it's important for us
- Data at GDPR
- What we are doing to get ready
- Our GDPR approach and new policies
- What we are going to need to do differently on an ongoing basis

- The main implications for David Phillips are:
 - Any contact data we keep needs to be accurate
 - We need to gain individual consent if we are to keep and use this data
 - We need specific granular consent on how we use the data
- And if we get it wrong.....
 - We can't contact our customers in future for sales or marketing reasons
 - Customers may not be able to work with us under the terms of their GDPR policy if we are not compliant.
 - Large corporates and Public Sector organisations will take their privacy responsibilities seriously
 - They will have onerous requirements – we will have to show we comply
 - The penalties for breaching the regulations are very stiff
 - Up to €20million!

- We keep a large amount of personal data
 - All of this needs to be GDPR compliant = policies, processes & systems

Whose data:

- Employees
- Potential employees
- Customers
- Tenants
- Developers
- Landlords
- Estate Agents
- Lead Sources
- Social & Care workers
- Contractors
- Concierge
- Client's neighbours
- Sub-contractors
- Vendors
- Introducers
- Indirect vendors
- Service suppliers
- Recruitment agencies

What data:

- Full names
- Photo ID
- Contact details including, phone numbers, address, email address
- Financial information - bank or card details, CCV numbers, potentially earnings
- VAT numbers
- Credit insurance details
- Photos of their property – inside and outside
- Door entry codes / key safes codes
- Contracts
- Some personal credit card information for employee expenses
- Reference checks

Where we store it:

- Email
- Nav
- On Microsoft packages (spreadsheets / word docs)
- Shared drives
- In a file – physical or electronic
- On a database
- TalkDesk
- Online payment systems
- Citrix
- iDesign
- Smartsheet
- USB sticks
- On MS Teams
- On work phones
- On personal phones
- Esendex
- ZenDesk
- Driver paperwork
- On paper or in notebooks
- Archive store rooms

- Many people may have access to the personal data
 - We need to ensure we all access, use & sharing is compliant

Who in David Phillips can see it:

- Outbound Sales
- Inbound Sales
- Customer Support
- Rental
- Finance
- Accounts Receivable
- Credit Control
- TOC
- Warehouse Admin
- Installers
- Projects
- WTF
- IT
- Stock
- Accounts Payable
- Buying & Merchandising
- Fitted
- Indirect Spend Team
- Window Treatments

What we use it for:

- Place orders
- Take payment
- Make deliveries
- Proof of delivery
- Proof of installation
- Invoice queries
- Arrange refunds
- Sales
- Marketing
- Requesting quotes from suppliers
- Making payments and refunds
- Checking credit limits
- Creating reports
- Reference checks

Who we share it with (outside David Phillips):

- Agents
- Sub-contractors / contractors
- Couriers
- Customers
- Landlords
- Relocation company
- Lead sources
- Insurance company - compensation claim
- Tenants
- Support workers
- Carers
- Lead sources
- Instagram
- Facebook
- Credit checks
- Contractors
- Suppliers

- Developing a GDPR Policy:
 - Policy Statement – our public-facing privacy policy
 - GDPR Policy – our internal document (giving formal details)
- Creating GDPR processes & procedures and updating existing ones
- Publishing a GDPR page on the website
- Setting up a campaign to obtain our contacts' consents as required
 - Giving them the opportunity to correct their data at the same time
- Updating NAV (and iDesign) with the contacts' consent status
- Appointing a Data Protection Officer (P J Goldsworthy)
- Setting up a support process

Updating our contacts details and permissions

- Email campaign starts on Friday 20th April
- All contacts will be asked to opt in, their options are:
 - You can contact me for sales and marketing purposes
 - If so, whether by phone, email or post
 - Hold my data only to deliver services – but no marketing
 - Delete my data
- The information will then be updated in NAV (and iDesign):
 - Anybody who opts out or does not respond will be deleted in the next periodic round of data-cleansing
- We'll chase customers who don't respond by email and then by phone

Our GDPR approach – Guiding Principles

- Our contacts trust us to keep their personal data secure and private
- Our overriding principle is that all personal data is confidential
- Data Protection Officer responsible for policy
- All are responsible for compliance
 - Data Protection Officer is accountable

- We hold the following types of personal data:
 - Company contact information
 - This is linked to customer & vendor data in NAV
 - NB also applies to individuals (i.e. legal entities)
 - Person contact information
 - Employee data
- Most of our data is used only for delivering our services
 - NB – don't need consent to use it for this purpose
 - But we do still need consent to retain it
- Where our data comes from:
 - Directly from individuals
 - From other companies
 - But only if sharing it fits in with their privacy policy
 - And only if we are compliant under their policy

Our GDPR Approach – Use of Data

- We use data to provide our services, including:
 - Photographs of installations
 - Processing payments
 - Credit checks
 - Marketing and sales purposes – if consent is provided
- We don't provide personal data to any third parties
 - Except subcontractors
 - And only if they are GDPR compliant
- Primary source of personal data is held in our NAV system:
 - Secure
 - GDPR compliant
 - Used by all – linked to iDesign

- We can **hold** personal data *only* if we have consent from the subject
- Without their consent, we can use their information *only* to **respond**
 - Including delivering any services they have bought
- We can **initiate** contact with our customers for sales or marketing reasons *only* if they have given us their consent to do so
 - And *only* by the means of communication to which they have consented
- We will be inviting all our contacts to consent
- If anyone **withdraws** their consent for us to hold their data:
 - We can no longer contact them for sales and marketing purposes
 - We must delete their data during the next periodic data cleansing

- Our contacts have the following **rights**:
 - To be informed of any personal information we hold on them
 - To ask to see the personal information we hold about them
 - To amend their data
 - To ask us how we are meeting our GDPR requirements
 - To change their consent on whether we hold their data and what we can use it for
- We are obliged to keep all personal data accurate and up to date
- We now have an email address for all GDPR queries:
GDPR@davidphillips.com

Our GDPR Approach - Responsibility

- We are *all* responsible for *all* personal data we collect, store or handle
 - We must ensure that all use complies with our policy – particularly sharing
- Some specific responsibilities include the following:

- | | |
|---|--|
| <ul style="list-style-type: none">• Exec Team<ul style="list-style-type: none">• Accountable for meet our legal obligations• Data Protection Officer<ul style="list-style-type: none">• Overall responsibility for Data Protection in David Phillips• Infrastructure Manager<ul style="list-style-type: none">• Ensure all IT systems, services and equipment are compliant | <ul style="list-style-type: none">• Marketing Manager<ul style="list-style-type: none">• Ensuring our sales and marketing campaigns are compliant• Head of HR<ul style="list-style-type: none">• Keeping our employee data secure and compliant• Data Owners<ul style="list-style-type: none">• Ensuring our contact data is accurate and consent is captured• Carrying out periodic GDPR data cleanses |
|---|--|

What you need
to know about
GDPR

GDPR at David
Phillips

GDPR and you

- Your responsibilities for keeping data safe
- What you need to do differently

Your Data Responsibilities

- Keep all personal data **secure**
- Access the personal data **only where you need it** for your work
- All personal data should be **entered only in a controlled environment**
- **Don't share personal data** - internally or externally - **unless**:
 - The person has a need to know
 - The recipient is GDPR compliant
 - You have validated their identity
- **Use up-to-date** personal data
 - From NAV or iDesign
 - Not from separate data you hold
- Regularly **review and update** all personal data you hold
 - If it's no longer required then delete it
- If you are unsure, ask your Line Manager
 - Or email GDPR@davidphillips.com

What you need to do differently



What you need to do differently – keep all data secure

- System data
 - Data should only be stored in:
 - NAV
 - David Phillips Office 365 – Outlook or OneDrive
 - Don't save data directly onto laptops or mobile devices
 - Don't keep any personal data on your personal devices
 - Own computers, phones or tablets, memory sticks, paper or notebooks
- Photos of properties should be taken on work phones
 - Any taken on a personal phone should be transferred to a work storage location and then deleted from the phone and cloud storage
 - And not uploaded on Facebook or Instagram unless the owner has consented
- Never capture payment card information
 - Don't note down on paper
 - Stop recording on TalkDesk

What you need to do differently – keep all data secure

- Hard copy data
 - Don't leave paper where other people can find it - keep a tidy desk
 - Keep information in a locked desk or filing cabinet – whether it's on paper or a USB memory stick
 - On disposal - shred any paper that contains any personal data
- Keep all your data current
 - If a contact wants their contact details removed, we need to remove it from all sources, including:
 - Spreadsheets or databases
 - Outlook or phones
- It is your responsibility to maintain your own records
 - Update regularly to reflect NAV/iDesign
 - Or delete
- If you get any requests to amend personal data, ask them to email
 - To GDPR@davidphillips.com
- Highlight suspected data breaches
 - This includes loss of phones, laptops or USB sticks with personal data on
 - David Phillips **has to investigate and externally report** the outcome of any data breach

- Setting up and amending customers:
 - When we set up new customers we need to obtain, and then maintain GDPR consent on NAV
- Impacts to sales calls:
 - We can still contact people regarding an order or a particular enquiry from a customer (sales order or warm lead)
 - If a contact hasn't opted in to receive marketing information by voice means we cannot call them (e.g. cold calls or following up for potential repeat business with historic customers)
 - It is a breach to contact anyone who has been introduced us to unless the contact has consented for the introducer to share their data with us
 - The Leads Tracker will need to be kept up to date regularly cleansed

How we need to manage our data differently Inbound Sales, Customer Support, Invoicing and Accounts Receivable Teams

- Setting up and amending customers:
 - When we set up new contact on NAV we must obtain and maintain GDPR consent
 - Due to the link between customers, person contacts, company contacts and billing information on Nav there is a process that will need to be followed before you update contacts GDPR consent
 - You will be given a script for updating and requesting permissions from customers
- Impacts to sales calls
 - We can still contact people regarding an order or a particular enquiry from a customer (sales order or warm lead)
 - If a customer hasn't opted in to receive marketing information by voice we can't contact them (e.g. cold calls or following up for potential repeat business with historic customers)
- Your involvement in the project
 - From 30th April, start asking for customers GDPR preferences
 - You will be the main people maintaining and updating the contact data
 - Update credit account application forms & reviews to incorporate GDPR consent

- Setting up and amending vendors:
 - When we set up new contacts in NAV we must now obtain and maintain GDPR consent information
- The process for setting up vendors is:
 - First set up the contact
 - Obtain consent to keep the data for transaction purposes only
 - We will not be selling or marketing to vendors

What you need
to know about
GDPR

GDPR at David
Phillips

GDPR and you

What next

- What happens if you get any queries from customers
- Where to find more information
 - Website
 - Policy
 - Procedures & Processes
 - Data Protection Officer
- Wrap up

- For further information, please refer to our policy documents:
 - Policy Statement – our public facing privacy policy
 - GDPR Policy – our internal document
- Support:
 - Data Protection Officer is PJ Goldsworthy
 - Helpdesk – GDPR@davidphillips.com
- Questions from customers:
 - If you get any questions from any customers, introducers or contacts on data or our GDPR approach the email should be forwarded to GDPR@davidphillips.com

And to finish.....

- What are your key learnings from this session.....
- What is the one action you will take to ensure we are GDPR compliant?

**Any Questions...
Just Ask!**





Showrooms

Central London

57 Rathbone Place, London, W1T 1JU

Manchester

Longwood Road, Trafford Park, Manchester, M17 1PZ

Emma Douglas

emma.douglas@davidphillips.com

Moblile: 07880 230 178

David Phillips Furniture Ltd

57 Rathbone Place, London, W1T 1JU

08451 088 088

davidphillips.com