DAVID PHILLIPS/

GDPR Frequently Asked Questions

Version	Final
Updated	17th May 2018
Produced by	GDPR Project Team
Authorised by	Data Protection Officer

For internal purposes only, not for circulation

Introduction

Thank you to everyone for being engaged with the new General Data Protection Regulations.
Here are the answers to the questions we've been asked so far.

Individual rights under GDPR

Some of our clients are vulnerable people; is there anything we need to do additionally for these people?
The GDPR principles apply equally to all people regardless of whether they are classed as vulnerable people. All their personal data is confidential and should be safeguarded and not shared. We do have contracts with customers whose residents are vulnerable people; these contracts will often have additional requirements which go beyond GDPR and need to be met – just as they are now.

Estate agents provide us with tenants' contact details for us to call to arrange access. Should we ask them if the tenant has given their permission to pass on their contact details? What happens if they haven't?
We do need to ask private landlords if the tenant has given them permission to share their contact details with us; if they tell us they have, then we can assume that is the case; if they haven't, then we should ask them to confirm with the tenant before they pass on their details.
The information is given to us in confidence, purely to fulfil the order and not for any other purpose, so we can use the information only for that one transaction.
We will contact all our account customers to obtain a document confirming they will obtain permission for any access contacts before they pass the details on to us.

Individual Rights Under GDPR - Sharing Data Externally

We sometimes deliver stock directly from the supplier to a client – what do we need to do regarding a GDPR permissions perspective?
Our policy states that our sub-contractors may fulfil orders where necessary and if they do, the sub-contractors have contractual obligations to meet our safeguarding requirements. This means we ensure all our suppliers are GDPR compliant and they need to treat any information we provide to them confidentially, use it only for the purpose of fulfilling the order and they must not share it.

If somebody asks us to send them any personal information, for example a copy of their invoice; what is the policy for validating their identity?
The information should only be emailed to one of the contacts on the customer account – and they need to have opted in. If they have not opted in, they will need to do so by sending an email from the relevant address to confirm their identity.
If you are asked to send it to another email address, you should ask for email permission from a valid (opted in) contact on the customer account. Once you have permission from a valid contact, you can send the information.
If the contact wishes to be entered on the system to avoid such validation again in future, they must opt in at least for Transaction purpose. For relevant customer contacts, we would normally wish to invite them to opt in for Marketing purpose too.

We sometimes pass the information of one supplier to another supplier; can we continue to do this, e.g. passing the details of a fabric supplier to an upholsterer?
Normally in these circumstances you will be passing on public information rather than personal data; in which case the information can be shared. If you are concerned it may be private information (e.g. mobile phone number or personal email) or commercially sensitive, then you will need to get consent from the person whose information it is under GDPR.
Regardless of GDPR, supplier information is considered to be 'commercial in confidence'. You must therefore ensure that you are authorised to share it to avoid breaching our confidentiality policy.
(The example here is one where it might be a permissible exception for the relevant staff.)

We are sometimes asked for supplier references – should we ask the supplier's permission before we pass on their contact details as references?
Yes, of course. But we should always ask permission before we use anybody as a reference as a matter of courtesy and professionalism – the reference may not be very positive otherwise!

If a customer or supplier would like to talk to a specific colleague (for example the Finance Director), should we pass on their contact details?
In general, you shouldn't pass the colleague's contact details on unless you have their permission to do so. Instead you should pass the customer or supplier information to the colleague to make contact. It is not a GDPR breach to pass on work contact information, but it is a courtesy to ask your colleague first.

Contacting Potential Clients

How do we find out whether a client has opted in to be contacted for sales or marketing purposes?
You must always check in NAV or iDesign before you contact any existing customers for 'cold' sales opportunities or for any marketing purposes. You can initiate an interaction for these purposes only if the contact has opted in to Marketing purpose – and then only by a method they have permitted. If they have not opted in to Phone, then you cannot call them to initiate contact.

We have been investigating organisations to target for potential business; can we proactively contact them to ask for a meeting?
The information on these organisations is in the public domain and is therefore not personal data and therefore outside of the scope of GDPR. You may contact these organisations for sales and marketing purposes.

Other Organisations' GDPR Compliance

Do we need to ask the organisations with whom we have Framework Agreements for their GDPR policies?
We don't need to see their GDPR policies. We should seek a statement from them confirming that they share personal data with us only where they have obtained the relevant consent. They would normally ask us to confirm that we will use the data only for the purposes provided and not for anything else. In most cases this already exists under the Data Protection Act – we are not asking them to opt into receiving marketing information, so we are already covered.

If we are referred leads from an introducer, how do we the ensure the person has provided their permission for us to contact them?
We will be obtaining contractual agreements from all our introducers that confirm they comply with GDPR and have obtained the subject's consent to pass on their personal data for the purpose of responding to the enquiry. Note that this does not give us permission to retain the data or use it for marketing purposes – only to follow up on the specific lead. We should therefore seek the subject's consent to hold their data, ideally for Marketing purposes.

How do we know if a company, contact or sub-contractor is GDPR compliant; we often work with one-man-bands?
We will be doing a review of all our suppliers to ensure they are GDPR compliant; we will need to cease trading with any that can't demonstrate that they are compliant.
We will send out a survey to all suppliers and introducers to ask them to confirm their GDPR compliance.
We will review our agreements with sub-contractors to contractually commit them to treat any personal data provided by us confidentially, use it only for the purpose of fulfilling the particular order, not retain it or use it for any other purpose and certainly not share it with any other party.

Keeping data safe – Hard Copy Data

We don't have anywhere to lock the driver paperwork away at night. Including floorplans with address information in pigeonholes. What do we do?
We need to ensure the information is kept safe, is not misplaced, is shared only with those people who have a reasonable need to know it and only to the extent reasonably required to fulfil the legitimate purpose. It is clearly appropriate for the installers to have this information. Managers need to ensure there are suitable arrangements to avoid the information being seen by those who do not need to know.

We don't have lockable drawers for our notebooks or paper on our desks. What do we do?
The best way to capture information securely is to save it on your system – either OneNote, email, in NAV, iDesign or anywhere else on 0365.
If you do write it down, you need to safeguard it, keep it confidential and destroy it as soon as it is no longer required. You can record it in a way that the data is impersonalised – e.g. use the person's initials when jotting down a phone number: which reduces the risk of a breach (and is quicker). We recommend shredding anything containing personal information at the end of the day. But it is much better to save it in O365 – that also saves paper (in accordance with our environmental policy).
Under absolutely no circumstances should bank details or card details be captured on paper.

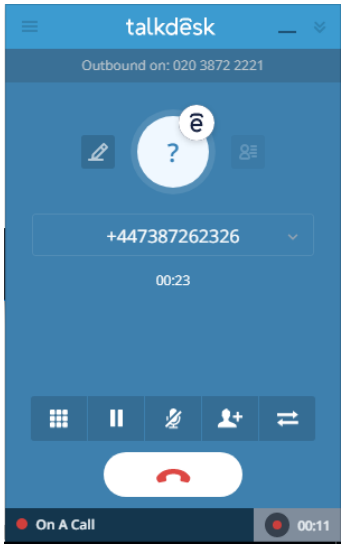
What are the expectations around locking away information. Do we need a safe at home? Or a locked drawer? Is it OK just to keep it in a locked house? This includes any personal data or property floorplans that contain address information.
It's OK to keep the information in a locked house; just keep it safe and confidential. Don't keep it any longer than you need it.
However, as for the question above, the best place to save it on a system.

We maintain lots of confidential documents, such as vendor forms, customer forms, invoices and statements. Do we need to store them in lockable cabinets? Do we need to keep hard copies, or can we scan them and shred the hard copies?
We don't need to keep hard copies of these documents; the most secure way of storing them is to scan them, put them safely on David Phillips secure systems and then shred them. If you do need to keep hard copies, then they should be locked away. The relevant managers need to ensure that there are suitable arrangements to safeguard any personal data.

The post tray often contains lots of personal information, do we need to do anything to secure it?
Confidential information, including customer statements, should always be treated as confidential and immediately put into envelopes.
The name and address on envelopes may also be personal information under GDPR. Whilst it is acceptable for post trays to be left out as now so that any person can put envelopes in them, it is rarely legitimate for anyone to look through the address information on the letters. No special arrangement needs to be made but staff and managers should challenge anyone looking through the mail just as they would an unaccompanied stranger in the office.

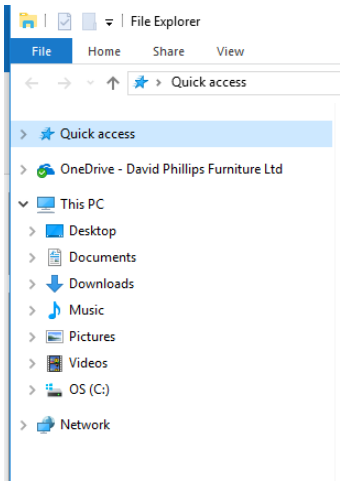
Keeping data safe – System Data

How do you stop recording on TalkDesk when you are taking credit card information over the phone?
You can stop recording whilst you are on a call by clicking on the button in the bottom right hand corner of the screen:



How do you save files onto OneDrive?

If you open up "File Explorer"  you will see the following view:



Just copy all your documents from your desktop into the "OneDrive – David Phillips Furniture Ltd" folder and delete it from your desktop. You should do this whether you have a laptop or desktop computer. This means the files are automatically backed up and there are numerous other advantages such as sharing for collaborative working.
If you have any questions, please email it-helpdesk@davidphillips.com

Are the scanned documents on the server kept securely?
Yes

We text or WhatsApp our drivers with contact details; should they delete these after delivery as part of the debrief process?
A process should be developed and put in place to delete this information on a regular basis. The drivers should never store contact details on personal phones, or use the contact details for any purpose other than to contact customers regarding a delivery.

All our mobile phones have the same PIN numbers, should we change them?
We should all change our PIN numbers and keep our phones locked when we are not using them.

Photographs of Installs

What is the policy on uploading photographs of installations to personal social media accounts?
Photographs of installs should **never** be uploaded to personal social media accounts – any that are already on your personal accounts should be removed immediately.

What is the policy on uploading photographs of installations to the David Phillips social media accounts?
Photographs should be uploaded to social media only if we have the explicit permission of the owner of the property. We need an auditable record of the consent to publish. Please refer to the policy and process for more information; we will need a central auditable record of the consent.
It will not be sufficient to add a "tick-box" to our terms and conditions, as you will need to show the photographs to the owners and gain approval to post the specific photographs.

Can we use of personal phones to take photographs of installations?
Photographs of installations should only be taken on David Phillips phones.

Our agents often ask for us to share pictures with them, can we do that without the owner's permission?
Under our policy, it is permissible to share the photographs with the agents either to demonstrate the installation the agent has asked for or to show any issues. If the agent wishes to use the photographs for any other purpose, they will need the consent of the property owner.

Deleting Records

Some of our products have long warrantees, what happens if a client who has asked for their details to be deleted then calls up with a question on a warrantee?
This data will be available on the archive system, we will be able to get the transactional information which we can use for this purpose. To get access, please log an IT Helpdesk request.

Credit Card and Bank Information

We receive credit card information from our customers via email which is often forwarded on to multiple people, should we continue to do that?
We should ask our customers to phone up with the credit cards and then capture the information directly into one of our payment systems – Stripe or SagePay.
If credit card information is sent by email, it should be deleted from all emails immediately once it has been used.