WORKING FROM HOME: MAINTAINING THE SECURITY AND PRIVACY OF PERSONAL DATA

Many businesses have now had their employees working from home for more than a year. While most have adjusted to the challenges and opportunities, this is a good time to remind staff of the importance of keeping vigilant to ensure that the personal data that they deal with in their work is kept secure and confidential and only used for the proper purposes.

If your business has one, the Data Privacy Officer (**DPO**) or Data Privacy Manager (**DPM**) should be able to answer any questions about data protection and to help to respond to issues like data breaches and subject access requests. If not, or if the query is more complex, then the Collyer Bristow Data Protection team is also available to provide advice or assistance on any issues or difficulties.

These are our top **six tips** on data privacy which will help to manage the risks relating to data protection under the UK GDPR and the Privacy and Electronic and Communications Regulations (PECR) while working outside the office.

1. DATA BREACH REPORTING

Since everyone is travelling far less, the risk of a physical data loss (files, laptop or phone) is significantly reduced. However, electronic data loss is still a high risk. If you realise you have sent an email or other communication to the wrong recipient, you should inform your DPO or DPM immediately after you discover the mistake. You should also send a fresh follow up email to the recipient (do not resend the personal data that caused the breach) as soon as possible and ask them to delete all copies of the email e.g. from their inbox, sent items and deleted items folders (preferably without reading it or any attachment) and confirm that they have done so. Your DPO or DPM will assess the risks arising from the data breach and advise whether the consequences of the breach are sufficiently serious that the Information Commissioner's Office will need to be notified. If so, this will need to be done within 72 hours of discovering the data breach.

You may have or wish to adopt a policy to inform customers and any other data subjects whose personal data has been inadvertently disclosed, even if you do not have a legal obligation under GDPR to do so. It is far better that your customers hear from you, rather than from an unintended recipient who chooses not to cooperate with you.

2. PERMITTED USES OF PERSONAL DATA

When personal data is collected, it is usually for one or more specific purposes. If you want to use that data for a different purpose, the new use needs to be considered very carefully to avoid committing a data breach.

For example, a customer or contact (Party A) may ask you for contact details of other customers or contacts (Parties B and C) in order to offer products or services to them or to pitch a business proposal. Unless you can prove that at the time when Parties B and C provided their contact details to you, or subsequently, it was clearly envisaged that they had an expectation that you may use their data for this further purpose, you should not do so. In this case you could contact Parties B and C and inform them of the request from Party A, asking for express consent for you to be able to pass on the contact details. Unless that informed consent is provided and you keep a record of it, you should not comply with the request.

This also extends to your own personal details. For example, a customer may ask for the home address of a staff member in order to send them a small birthday gift. This may seem a harmless request, but unless the intended recipient has given express consent for their home address to be shared, you should not do this. Any gift will in any case have to comply with your Anti-Bribery policy.

3. UNSOLICITED CVS

If you receive an unsolicited CV containing personal data (rather than anonymised details) from a recruitment agent, you should delete it without reading any attachment. The recruiter is probably in breach of its privacy obligations and is likely to be abusing its position as a data controller in an attempt to drum up business.

4. DATA SUBJECT ACCESS REQUESTS (DSARS)

Be on the lookout for these. If any individual contacts any member of staff asking what information your business holds about them, no matter how the request is made, it is essential to notify your DPO or DPM immediately. DSARs can be oral or in writing and do not need to specify that they are DSARs in order to be one. There is a 30 day time limit for responding and a detailed investigation and search may need to be carried out, so the sooner the request is passed to the correct person to respond, the better. You should have a procedure for dealing with DSARs which will include steps to verify the identity of the requester to ensure that they are entitled to the information they seek.

5. MARKETING

As part of complying with UK GDPR and PECR, your marketing lists will have been reviewed so far as possible to ensure that recipients have either given consent to being marketed, or have received identical or similar goods or services from you so that marketing is permitted.

Do not be tempted to "carpet bomb" a wider range of contacts with marketing material. You need to have either express consent or another valid legal basis.

In addition, if anyone contacts you to say that they do not want to receive any more marketing material either at all, or on a particular subject, be sure to make a note on your marketing database to remove them either from all lists or those in which they are no longer interested and keep a record of the relevant names and contact details on a "Stop List".

6. SCAM CALLS AND EMAILS

Continue to be on high alert if you receive a request for information or a request to make a payment which looks a little odd. Fraudsters have become more active than ever during the lockdown and are always trying to exploit someone trying to be "too helpful" in providing information or redirecting a payment. Even if a request looks genuine, do not hesitate to double check through separate channels.

If they are a contact, ring them using a number from your previously saved data – do not use a phone number in a suspicious email. Do not reply to a suspicious email: send a separate one to the person making the request or preferably speak to them. If you get an email address for a sender which looks genuine, but the content is odd, you can try hovering over the email address which will often reveal the full details. If it is not the real person then the actual email address is probably different.

Take extra care also where email addresses look the same, but are in fact one letter or character different, or for example where the email address is ".com" rather than ".co.uk" or from "petr.smith", instead of "peter.smith", which is the one you usually see. If in doubt, contact your IT team, your DPO or your DPM.

FURTHER HELP

If you need any further help on these or any other Data protection matters, please contact either **patrick.wheeler@collyerbristow.com** or **howard.ricklow@collyerbristow.com**.