**Five key UK GDPR considerations when implementing new technology in your practice**

Using new technology, particularly in a time of increased cybercrime, does bring risks and requires updates and amendments to be made to existing UK GDPR compliance frameworks that you have in place now, not later.

**We have prepared this guidance and assessment tool to help business owners work through a process to assess new technology products from a UK GDPR compliance viewpoint.**

1. **Firstly, are you processing personal data under the UK GDPR?**

Using technology products such as Zoom, Skype or Microsoft Teams to communicate with your customers or employees, exchanging the face to face experience for a virtual meeting or consultation, does not automatically mean you have to worry about the UK GDPR. Having an appointment or meeting with a client, employee or another data controller in which personal data is disclosed is not in itself data processing. By the same rationale, using various technologies simply as a means of hosting a meeting, does not equate to processing personal data.

In short, if you have a live conference or meeting via video, this is no different to a phone call or a face to face meeting and you should apply the same confidentiality boundaries you usually would.

However, where you record the personal information in note form, or elect to record the meeting by recording technologies such as video, transcript recording, instant messaging, whiteboards, or the sharing of files in chatrooms or via other share files technologies, such actions **do** amount to data processing activity and should trigger additional considerations in relation to your UK GDPR compliance.

**Checklist**

1. Are you processing personal data?
2. If yes, what form does this take? Notes, video recordings etc.?
3. **Are you sharing personal data with third party providers?**

Where you and others use apps such as Zoom and Skype, personal data pertaining **to you and other users,** such as your IP address, location data, and device information, will likely be shared with the third-party provider. These third-party providers may potentially share this information with other parties in turn. You should therefore carefully review the privacy policy of the provider to ascertain if your data is shared with other third parties.

Where you elect to record the call either by video or transcript or sound recording, or use cloud-based technologies to store data, you are a d**ata controller** sharing client or employee **data** with Data Processors and the UK GDPR requires that you enter into data processing agreements with these parties, as you do with other suppliers you work with.

Global technology companies will not enter into bespoke data sharing agreements drafted by data controllers. Where you decide to use a certain app, you should check their website for a copy of their data processing agreement or request a copy.

Zoom, for example, publish their version of the data processing agreement for acceptance by their users [here.](https://support.zoom.us/hc/en-us/articles/360000789323-Data-Processing-Addendum)

Ensure that you have a data sharing agreement in place with all your data processors.

**Checklist**

1. Have you checked all privacy settings in the technology product?
2. Have you located and reviewed the Data Sharing Agreement offered by the tech company?
3. Does the data sharing agreement meet your requirements?
4. Is your data, or that of your client/employees shared with any other 3rd party by the tech company?
5. **Where in the world do these third-party technology companies store data?**

**Under the UK GDPR,** you may only transfer personal data to a third country or an international organisation outside of the UK where there are appropriate safeguards in place, or a relevant exemption applies. Storage of your data is an international data transfer where data centres are located outside the UK. Consider the following steps:

1. Verify where, geographically, your data will be stored – check the privacy statement or research the company. You can always check directly with the organisation prior to sharing data and record the response;
2. If the data centre is located outside the UK, you will need to check if that third country is on the adequacy list. That is countries outside the UK that are considered to have adequate data protection regulations.
3. In relation to companies or data centres located in the US, as the US Privacy Shield is no longer valid you will need to source additional safeguarding measures where you have relied upon the Privacy Shield historically.

and;

1. There are other safeguards available such as Standard Contractual Clauses or SCCs which can also be agreed with organisations who fall outside the remit of the categories above. The SCCs will be formally amended in 2021. Where you have relied upon a SCC historically, this will need to be amended. You will also be required to conduct a risk assessment in relation to the national data protection legislation and protections within the country that you are transferring the data to. Checks should be made directly with the organisation and advice sought where necessary.

 **Checklist**

1. Where, geographically, is your data stored by the tech company?
2. Have you checked which safeguards are in place? Adequacy decision/ /SCC’s?
3. Have the SCCs been amended?
4. **What security does the technology company provide for personal data?**

The sixth principle of the UK GDPR requires you to take ‘appropriate organisational and technical measures’ to secure the integrity of all personal data you are processing.

Whatever new technology you decide to use, it is critical that you ensure that the security of the data you are processing is not compromised by the use and integration of these technologies into your systems. It is critical therefore to ensure that you have:

* maximised the security and privacy settings with each product;
* verified your own security, ensuring it is current and sufficiently robust; and
* taking all best practice measures to ensure you have not given unauthorised access to any individual.

It is commonly assumed that ‘cloud hosted’ products are insecure or prohibited - far from it. Large businesses such as Microsoft (which owns Skype), Google and Dropbox spend billions of dollars ensuring the security of their systems. Provided the privacy setting, geographical location of data and terms of data processing agreements meet your requirements, you can use these and many more similar products to process personal data.

If you have concerns about *the IT security* aspect of any product, it is worth contacting your usual IT adviser to get their advice.

1. **Your Compliance Framework - Update your UK GDPR Documentation**

1. **Privacy Policy**: In adherence to the first principle of the UK GDPR there is an ongoing responsibility for the Data Controller to ensure all data processing is lawful, fair and transparent. To satisfy this responsibility, when electing to use technology which you may use currently or in the future, it is essential to update your privacy policy to reflect this.

In the section entitled ‘We may share your data with...’ you should include the list of all providers for applications that you use in the course of your business. Similarly, if the use of this app results in the transfer of data outside the UK, you should stipulate this and the associated safeguard you are relying upon.

2. **Third-Party Data Sharing Register**: We have already outlined the requirements to have a data sharing agreement in place. Ensure that when you commence use of new technology, you add the name of the provider as a third party where relevant, keep a copy of the Data Processing Agreement for your records and check back for any updated versions of the agreement, at least annually.

3. **Data Retention Policy:** When sharing data with a third-party provider, check their privacy policy or the data sharing agreement to ascertain how long they will retain any personal data they are processing on your behalf. Make sure this is reflected in your own data retention policy.

4. **Data Protection Impact Assessment** **(DPIA):** You must complete a DPIA where you are processing special category data and records **on a large scale**, if such activity is **likely to result in a high risk** to individuals.

**Checklist**

1. Have you updated your Privacy Policy?
2. Have you updated your Data Retention Policy?
3. Have you updated your Data Sharing Register?
4. Do you need to carry out a DPIA?

**Conclusion**

We hope this assessment tool provides you with a workable structure to help assess new technology products from a UK GDPR perspective and rather than being fearful of security or data protection issues, that you’re empowered to embrace the opportunity that technology brings to help make your business more efficient and robust.