SPRING NORTH

COLLABORATION + INNOVATION = IMPACT

Golden Rules to sharing information

1. FIND OUT WHERE THE PERSONAL DATA IS

This is the first and one of the most fundamental steps. Personal data is "any information related to a natural person or 'Data Subject' that can be used to directly or indirectly identify the person". Once you know where all of the personal data is located, you can find out who has access to it, how it is processed, where it has come from and begin to put in safeguards to become GDPR compliant. If you haven't done so already, do this as soon as possible.

2. MANAGE AND MONITOR THE SUPPLY CHAIN

Make sure you're aware of the data you're sharing and ensure compliance from any third parties. In most circumstances each third party that has access to your data should provide you with a legal and contractual agreement to protect the rights of data subjects. This includes those outside of the EU, any organisation that processes an EU citizen's data must be compliant with this legislation, irrelevant of their own jurisdiction.

3. MINIMISE DATA AND IMPLEMENT STRICT RETENTION POLICIES

Ensure you only hold the data you require and that you have a process for erasing old data you no longer need.

4. IDENTIFY ALL RELEVANT LEGISLATION – NOT JUST THE GDPR

Make sure you are aware of all legislation that affects the data you hold; for example, other legislation may require you to hold data for a particular length of time after its use – this would be a legitimate reason under the GDPR for you retaining that data.

5. CONTROL ACCESS TO THE INFORMATION

Ensure that only those who need access to the data have that access, and that this access is justifiable and appropriate.

6. ESTABLISH AND DOCUMENT A LEGAL JUSTIFICATION FOR PROCESSING

In order to process data you must have a lawful basis to do so which is clearly documented. There are six available bases under GDPR; these bases

can be found in Article 6, they include consent, contract, legal obligation, vital interests, public task and legitimate interest.

7. INFORM DATA SUBJECTS OF WHAT YOU'RE DOING WITH THEIR DATA & WHO HAS ACCESS TO IT

The data subject generally has a right to know why personal data is being processed about them, what data is processed and who processes it. You need to explicitly inform data subjects of the specific purpose that you are processing their data for and you shouldn't deviate from this without good reason. It should also be clear who they can contact about the data that is held about them.

8. HAVE AN INCIDENT RESPONSE PLAN

Should you suffer a breach to any personal data that you may hold, an organisation with an effective Incident Response Plan (IRP) is in the best position. This is likely to reduce the time it takes to find out you have a breach and therefore, reduce the potential loss of data and / or damage to your organisation. Within this IRP ensure you include your breach notification process - Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

9. DON'T BUY OR SELL BULK DATA SETS

This isn't a requirement of the GDPR but we'd suggest you avoid bulk data sets if possible. The intention of the GDPR is to give EU citizens more control over their data so the sale or purchase of bulk data must be very closely controlled or is likely to contradict that objective.

10. REMEMBER COMPLIANCE IS ONGOING

Once you have implemented the necessary controls and measures you are part way there but maintaining compliance is an ongoing requirement and requires continual management control. Think about establishing roles and responsibilities which include GDPR