phonovation

Questions to consider on your road to GDPR compliance

01.

DATA INVENTORY

What personal data does your organisation gather, store and from whom do you receive this personal data?

02.

DATA CLASSIFICATION

Have you classified the diverse types of personal data your organisation collects, controls and/ or processes?

03.

LAWFULNESS OF PROCESSING - Article 6

How did your organisation obtain this personal data and for what purpose has this personal data been collected/accessed?

04.

CONDITIONS FOR CONSENT - Article 7

Where processing is based on consent, can your organisation demonstrate that the data subject has consented to processing of their personal data?

05.

DATA MINIMIZATION - Article 23

Are you collating, managing and processing only necessary data?

06.

DATA PROTECTION POLICIES- Article 25

Does your organisation have adequate policies and procedures in place for processing personal data, storing personal data, transferring personal data, retaining/destructing personal data?
Do you need to review and update your organisation's existing Data Protection Policy, Privacy Statement and Privacy Notice?

phonovation

07.

RECORDS OF PROCESSING ACTIVITIES – Article 30

Has your organisation created a data processing log to maintain a record of all categories of processing activities under your organisation's responsibility or carried out on behalf of a controller?

08.

RIGHT OF ACCESS BY THE DATA SUBJECT – Articles 15 & 20

Can your organisation provide information to data subjects in a transparent and speedy manner, and without charge?
Can your organisation process data portability requests in a timely and appropriate manner?

09.

RIGHT TO RECTIFICATION AND RIGHT TO ERASURE – Articles 16 & 17

Can and/or does your organisation update the personal data that you store, hold, collect, maintain? If so, then how is this done and how often do you do this?
Can your organisation erase or remove personal data from use if requested?
How will your organisation do this if you have already made the personal data public?

10.

SECURITY OF PROCESSING – Article 32

How secure is your organisation's personal data?
Is access to your technology and manual files restricted to authorised staff only?
Are your computer systems and servers password protected and/or encrypted?
Has your organisation implemented appropriate technical and organisational security measures?

11.

REPORTING DATA BREACHES – Articles 33 & 34

Has your organisation put adequate policies and procedures in place in the event of a data breach?
Who would you contact and what would you do if the personal information that you were handling was stolen or publicly disclosed?
Can your organisation notify all relevant parties of a data breach within the mandatory 72 hours?

12.

DATA PROTECTION OFFICER – Article 37

Have you identified if your organisation needs to appoint a DPO, and if so who?