GDPR COMPLIANCE - A FIRST ASSESSMENT QUESTIONNAIRE (*)

The Belgian Privacy Commission CVPV/CBPL recommends that all **C**ontrollers and **P**rocessors maintain records concerning their processing of personal data – even if they are not obliged to do so under Article 30 GDPR.

Practically that means you should have a picture of the data flows within your organisation. Ask yourself – for what purpose(s) is personal information obtained, used and retained? Who will it be shared with? There may be several purposes – **analyse each such purpose separately**.

Processing overview - Analyse the information you hold?

- **Why** is personal data processed? (e.g. Staff admin, legal obligations, provision of goods or services, direct marketing, profiling …)?
- **Whose** personal data is processed? (e.g. Staff, clients, business contacts, suppliers, children … Source of data: individual themselves, third party source …)?
- **What** personal data is processed? (e.g. Personal details e.g. – name, address, e-mail, IP address, telephone, date of birth, financial details – bank account, credit card, tax reference, employment details {specify}; Special categories e.g. health, biometrics, criminal records)?
- **When** is personal data processed? (Includes obtaining, disclosing, storing, deletion ... e.g. When is it obtained? To whom is it disclosed *and* why? How long is it retained)?
- **Where** is personal data processed? (e.g. Electronic records – are they managed in house or by an external hosted service? Are the servers within the EEA, USA, or elsewhere? Cloud services – where are the servers? Manual records – location)?

Company processes

- Have you conducted staff training on DP? Who is your DP lead? Have you established guidelines/policies on DP both internally (employees) and externally (for clients/ customers/suppliers)? When were these last reviewed? What DP / 'Cookies' notices are there on your website?

Third parties

- Are you a **C**ontroller, do you hire external **P**rocessors? Have you got copies of the contracts? Have you reviewed them in light of GDPR requirements including security, integrity and confidentiality?

Transparency

- Did you up-date fair processing information that is provided to data subjects in clear language and taking account of the information mandated by Articles 13 & 14 GDPR?

Risk assessment

- Is there a regular process in place for testing and assessing your data management system for security and protection against both internal and external attacks?

Preparedness

- Is there an internal process for assessing and keeping a record of (and if necessary reporting on) any data incidents?

International

- If you transfer personal data across-borders outside the EEA have you verified what legal basis you are relying to carry out such transfers?