GDPR Key Concepts and other facts you need to know…

"Not one cap fits all" and the words appropriate and proportionate abound in GDPR parlance. However, it should be recognised that, while it is all about privacy, it is not just about Confidentiality. The rights of the citizen include that data be accessible in the right format (Availability) and that it is maintained and accurate (Integrity). It is worth noting that IL7 has a depth of experience in Risk Management and Accreditation Documentation Sets (RMADS) for both MOD and Central Government. For many organisations data security is about protecting operational viability and with MOD the physical security of its personnel and infrastructure. With the Police (IL7 spent 4 years with the Met Police and other forces, specialising in counter terrorism intelligence systems) it is the protection of information for operational and evidential purposes (as well as protecting their officers!). Within digital government and on-line services to the public, privacy is King. Yes, nobody wants downtime, but Data Loss Protection is more about citizens' rights than the ability to wage war on the criminal or adversary. The old RMADS no longer suits all situations and IL7 has developed a more privacy centric risk management process that is appropriate to HMG whilst it retains its capability to write RMADS based on CIA for operational and investigatory viability.

Five key concepts.

1. The Rights of citizens (natural persons – data subjects)
    a) To know what's going to be done with the data.
    b) To have copies of data.
    c) To correct data that is incorrect.
    d) To have data erased if there is no reason for it to be collected/stored – right "to be forgotten"
    e) To restrict processing – that is to deny processing and profiling for marketing purposes.
    f) To request data in digital format and the right to transfer this data to another supplier – data portability.
    g) Right to object to processing.
    h) Right to deny automated processing and to insist on human involvement in processing.

For more information go to https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/

2. Data Controllers should themselves 'do security well' and ensure any contracted/delegated Data Processors 'do security well'. This means they should employ:
    a. Appropriate technical and organisational measures should be employed.
    b. These should be proportional to the evaluated risks resultant from an agreed Risk Assessment exercise.
    c. Areas to be considered include:
        i. Maintain a holistic map of data flows, imports, exports and processing with the Asset inventory.
        ii. Encryption and Pseudonymising.
        iii. Physical, Personal, Procedural & technical controls to protect CIA.
        iv. Regular testing of the data processing oversight.
3. Legality and Consent.
    a. Ensure there are watertight business reasons for requesting data and this (and what is to happen to PII once given) is conveyed to the data subject in unequivocal terms.
    b. Ensure that, if business is reliant on consent, that it is asked for in unambiguous terms and if not unambiguously granted, collection, processing, storage and onward transfer are unequivocally ceased.
    c.
4. Accountability & Compliance.

a. Ensure there is a governance structure set up with a Data Protection Officer as the single point of contact.
b. Clearly define the boundaries between data controller and data processor. If you are the controller, although the processor has responsibilities and obligations under GDPR that were not so visible under DPA, you must contractually oblige the processor under SLA or KPI or whatever means you can, to 'do security well', maintain accessibility to data subjects to their data and to have an incident (breach) reporting/handling schema that dovetails to your own. If you are the processor you are well advised to ensure this is the case.

5. Privacy by Design and by Default.
    a. The main point here is that all new systems must be designed to be secure, to prevent unlawful access, alteration or deletion. New systems must be designed to allow citizens access to their own data, to amend where warranted and to request portability or erasure where appropriate.
    b. The design of new systems must incorporate the security enforcing functionality to maintain the level of privacy required through Personnel, Physical, Procedural and Technical controls.
    c. A risk assessment is required to ensure controls are proportional to need. A DPIA should be conducted on all new systems (see below).
    d. All legacy systems should be systematically subject to a Data Protection Impact Assessment (DPIA). This should include:
        i. Data Inventory and Classification.

ii. Data Flow Mapping.
iii. Privacy Impact Assessment.
iv. Review of Integral controls.
v. Review by GDPR SME.
vi. Recommendations of GDPR SME.
vii. Corrective Action Plan.
viii. Security Case for a ‘Licence to Operate’.
ix. Documented senior management acceptance.