VADEMECUM LPD
"COME ADEGUARSI ALLA NUOVA LEGGE SULLA PROTEZIONE DEI DATI"

1. Eseguire una **mappatura scritta** del trattamento attuale dei dati personali da parte del Titolare del trattamento (colui che determina lo scopo e i mezzi del trattamento), specificando quali dati personali vengono trattati, con quali finalità vengono trattati, chi tratta i dati, in che maniera vengono trattati (raccolti, trasferiti, conservati, restituiti, distrutti, ecc.), chi ha accesso ai dati, a chi i dati vengono comunicati, ecc. Per quanto possibile conviene eseguire la mappatura in un unico documento scritto, in maniera chiara, conservandolo e aggiornandolo in caso di modifiche.

2. Verificare se vengono trattati **dati personali degni di particolare protezione**, ossia dati personali riguardanti opinioni o attività politiche, religiose, filosofiche o sindacali, la salute, la sfera intima, l'appartenenza a una razza o etnia, dati genetici o biometrici, nonché dati relativi a perseguimenti o sanzioni amministrativi e/o penali, ma anche misure d'assistenza sociale. Occorre poi determinare se tali dati personali degni di particolare protezione vengono trattati su **vasta scala** oppure no.

3. Verificare se vi è una **profilazione** (trattamento automatizzato di dati personali per valutare e prevedere determinati aspetti personali, come ad esempio il rendimento professionale, la situazione economica, la salute, l'affidabilità, le preferenze, ecc.) oppure una **profilazione a rischio elevato** (profilazione con rischio elevato per la personalità o i diritti fondamentali della persona).

4. Verificare se vi sono delle **decisioni individuali automatizzate** (decisioni basate esclusivamente su un trattamento di dati personali automatizzato che comportano effetti giuridici o conseguenze significative).

5. Verificare se i dati personali vengono **comunicati all'estero** e in tal caso specificare in quali paesi (prendendo misure adeguate in caso di paesi a rischio, tenuto conto della lista dei paesi sicuri e di quelli non sicuri elaborata e aggiornata dal Consiglio federale; v. relativa ordinanza).

6. Verificare se occorre procedere con una **valutazione d'impatto** sulla protezione dei dati personali (quando il trattamento può comportare un rischio elevato per la personalità o i diritti fondamentali; per esempio, in caso di trattamento su vasta scala di dati personali degni di particolare protezione oppure di sorveglianza sistematica di ampi spazi pubblici).

7. Valutare se conviene designare un **Responsabile** del trattamento dei dati (colui che tratta i dati personali per conto del Titolare del trattamento; N.B. il dipendente che tratta i dati per conto del datore di lavoro non è considerato un responsabile).

8. Valutare se conviene designare un **consulente** per la protezione dei dati (non obbligatorio, bensì semmai opportuno).

9. Verificare se vi è l'obbligo di tenere un **registro delle attività di trattamento** (non obbligatorio per imprese con meno di 250 collaboratori i cui dati personali trattati comportano soltanto un rischio esiguo di violazione della personalità).

10. Esaminare sotto il profilo tecnico-informatico (hardware e software), ma anche fisico (fascicoli, schedari, locali, ecc.) e organizzativo (metodologia), se la **sicurezza del trattamento** dei dati personali è sufficientemente garantito. Ciò presuppone che occorre esaminare quali misure sono

attualmente messe in atto per garantire la sicurezza e in particolare: una corretta conservazione dei dati, misure per evitare perdite, soppressioni, violazione e furti dei dati personali, ma anche accessi ai dati personali da parte di persone non autorizzate. Ciò presuppone che vanno se del caso prese **misure tecnico/organizzative supplementari** per garantire la sicurezza.

11. **Formare** in maniera adeguata sulla protezione dei dati ogni persona che tratta dati personali o, anche, semplicemente ha accesso a tali dati. Occorre inoltre redigere e mettere a loro disposizione **direttive interne** sul trattamento dei dati personali.

12. **Informare** in maniera chiara ed esaustiva ogni persona i cui dati personali vengono trattati, in particolare sul tipo di dati personali, sulle finalità e modalità di trattamento, nonché sui loro diritti. Tale informativa avviene per il mezzo di dichiarazioni/informative sulla protezione dei dati (cosiddette privacy policy), per ogni tipo di trattamento, tipicamente per quanto concerne il trattamento dei dati personali di clienti o potenziali clienti, segnatamente per il tramite del sito web del Titolare del trattamento ("privacy policy"), ma anche tramite i cosiddetti cookie utilizzati dal sito web del Titolare del trattamento ("cookies policy") o qualsiasi altra modalità fisica/cartacea. Medesima o analoga informativa è necessaria per i dipendenti del Titolare del trattamento (nel contratto di lavoro, direttive o regolamento aziendale), per i fornitori, subappaltatori, e ogni altra terza persona i cui dati personali vengono trattati o a cui vengono comunicati (tramite specifiche privacy policy o richiamo alla privacy policy principale).

13. Predisporre **istruzioni** semplici e chiare per rispondere senza ritardo alle richieste legittime delle persone i cui dati personali vengono trattati (diritto di accesso, diritto di consegna, diritto di rettifica, diritto di cancellazione o distruzione dei dati personali, diritto di proibire il trattamento).

14. Predisporre **istruzioni** semplici e chiare per agire in maniera corretta e rapida in caso di violazione della protezione dei dati personali (rivolgendosi in particolare all'Incaricato federale della protezione dei dati e della trasparenza).

15. Prevedere la **soppressione o anonimizzazione** dei dati personali non appena questi non siano più necessari allo scopo del trattamento iniziale.