NUOVE DISPOSIZIONE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (PRIVACY)

A decorrere **dal 25 maggio prossimo** il Regolamento europeo n. 679 del 27 aprile 2016 sarà obbligatorio in tutti i suoi elementi nonché direttamente applicabile in ciascuno degli stati membri.
Dal momento che l'entrata in vigore del nuovo regolamento comunitario non comporterà l'abrogazione automatica della legge statale in materia di privacy (D. Lgs. 196 del 2003), il governo è stato delegato ad adottare uno o più decreti legislativi per adeguare il quadro normativo nazionale alla norma comunitaria, abrogando espressamente le disposizioni incompatibili. In assenza di provvedimenti legislativi in tal senso, troverà comunque applicazione il Regolamento europeo, quale norma prevalente.

A) DISPOSIZIONI CHE RIMANGONO SOSTANZIALMENTE INVARIATE RISPETTO ALL'ATTUALE CODICE PRIVACY

a) **Ambito di applicazione (art. 2 Reg.):** il Regolamento si applica al trattamento non automatizzato, automatizzato o parzialmente automatizzato di dati personali, con esclusione dei trattamenti di dati personali effettuati da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con una attività di impresa o professionale.
b) **Definizioni (art. 4 Reg.):** rimangono sostanzialmente immutate le definizioni di dato personale, trattamento, titolare e responsabile del trattamento;
c) **Principio di liceità (art. 5 Reg.):** si conferma che i dati personali devono essere trattati in modo lecito e corretto, per finalità determinate, esplicite e legittime, conservati per un arco di tempo non superiore al conseguimento delle finalità e trattati in modo da garantire una loro adeguata sicurezza.
d) **Base giuridica (art. 6 Reg,):** il trattamento è lecito solamente se l'interessato ha espresso il consenso, oppure se il trattamento è necessario per l'esecuzione di un contratto o precontratto di cui l'interessato è parte, per adempiere un obbligo legale, per la salvaguardia di interessi vitali dell'interessato o altra persona fisica, oppure per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, prevalente rispetto al diritto di protezione dei dati dell'interessato.
e) **Consenso (art. 7 Reg.):** il consenso deve essere informato, specifico, libero ed inequivocabile. Non è richiesta la forma scritta, ma il titolare deve dimostrare che l'interessato ha prestato il consenso ad uno specifico trattamento.
f) **Dati sensibili (art. 9 Reg.):** i dati relativi all'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, i dati relativi alla salute o vita sessuale o l'orientamento sessuale di una persona possono essere trattati solamente nei seguenti casi: a) se l'interessato ha prestato il proprio consenso esplicito (scritto), b) se il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti del

titolare o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale, c) per tutelare un interesse vitale dell'interessato o di altra persona fisica quando l'interessato si trovi nell'incapacità fisica o giuridica di prestare il consenso, d) se è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro, che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi i membri, ex membri o persone che hanno regolari contatti con tali enti e che i dati non siano comunicati all'esterno senza il consenso dell'interessato, e) se è necessario per finalità di medicina preventiva, medicina del lavoro, valutazione della capacità lavorativa del dipendente ovvero gestione dei sistemi sanitari e sociali. Il Regolamento, a differenza del codice privacy, non prevede l'obbligo di autorizzazione da parte del Garante per il trattamento dei dati sensibili (a tale riguardo occorre precisare che ad oggi il Garante ha esplicitamente autorizzato con specifici provvedimenti il trattamento dei dati sensibili, tra l'altro, nei rapporti di lavoro e quello effettuato da parte di organismi di tipo associativo, stabilendo le condizioni perché ciò possa avvenire, nell'interesse della persona fisica). Occorrerà verificare se il Garante, alla luce delle nuove norme europee, manterrà le autorizzazioni generali ad oggi applicate.

g) **Informativa (artt. 12,13,14 Reg.):** il titolare del trattamento deve fornire all'interessato tutte le informazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, per iscritto o altri mezzi, anche elettronici. Se richiesto dall'interessato (novità introdotta dal Regolamento europeo) le informazioni possono essere fornite oralmente, purchè sia comprovata con altri mezzi l'identità dell'interessato. **I contenuti dell'informativa sono in parte più ampi rispetto a quanto previsto dal Codice privacy; comunque, devono obbligatoriamente essere fornite all'interessato le informazioni relative all'identità e i dati di contatto del titolare e, ove nominato, del responsabile del trattamento, le finalità del trattamento nonché la base giuridica del trattamento e gli eventuali destinatari (tra cui l'indicazione dell'eventuale trasferimento dei dati in Paesi terzi). Una volta ottenuti i dati personali, occorre fornire ulteriori informazioni quali il periodo di conservazione dei dati oppure i criteri utilizzati per determinare tale periodo, i diritti dell'interessato (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione), il diritto di proporre reclamo ad una autorità di controllo, le conseguenze della mancata comunicazione dei dati, l'esistenza di un eventuale processo decisionale automatizzato, compresa la profilazione (novità introdotta dal Regolamento europeo).**

h) **Diritti dell'interessato (artt. da 15 a 22)** Come già previsto, è riconosciuto all'interessato il diritto di accedere ai dati personali, ottenerne la rettifica o la cancellazione, ottenerne la limitazione al trattamento o opporsi allo stesso, proporre reclamo all'autorità di controllo.

B) NUOVE DISPOSIZIONI

a) **Valutazione dei rischi e misure per garantire la sicurezza (artt. 24-25-28-29-32-40-41-42-43 Reg.)**: sulla base del principio della responsabilizzazione, il

titolare del trattamento analizza i rischi inerenti al trattamento, quali la distruzione, la perdita, la rivelazione, l'accesso non autorizzato, che potrebbero causare un danno all'interessato ed adotta le misure ritenute idonee per limitare tali rischi (principio della privacy by design). Quindi, a differenza di quanto avviene attualmente, non saranno sufficienti obblighi generalizzati di adozione di misure minime di sicurezza (previsti dall'allegato B al codice della privacy) in quanto tale valutazione sarà rimessa, caso per caso, al titolare ed al responsabile ove nominato in rapporto ai rischi specificatamente individuati. Inoltre, devono essere messe in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (principio della privacy by defoult). Infine, il titolare deve garantire ed essere in grado di dimostrare che il trattamento dei dati personali avviene nel rispetto delle norme (principio di rendicontazione). A tale riguardo, il Regolamento (art. 40-41-42-43) prevede la possibilità di avvalersi di specifici codici di condotta o schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate tenendo in considerazione le esigenze specifiche delle micro, piccole e medie imprese, fermo restando che l'Autorità garante, facendo anche riferimento alle prescrizione contenute nell'attuale codice della privacy, provvederà probabilmente a definire una serie di lenee giuda o buone prassi da adottare per la stesura di tali documenti. Il codice di condotta deve essere approvato dall'Autorità Garante ed il controllo della conformità è demandato ad un organismo di certificazione accreditato, anche se, allo stato, non è chiaro a chi verrà affidato tale ruolo, né sono definiti i requisiti per l'accreditamento degli organismi di certificazione e i criteri di certificazione.

b) **Registro delle attività di trattamento (art. 30 Reg.):** Il titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità; sono esonerati da tale adempimento le imprese od organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa rappresentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa dati sensibili o i dati personali relativi a condanne penali. A tale riguardo, il Garante ha intenzione di elaborare un modello semplificato di registro, da mettere a disposizione sul proprio sito, che i singoli titolari potranno integrare in base alle loro realtà specifiche e comunque utilizzare per avere in azienda un documento da sottoporre agli organi di vigilanza nel caso di eventuali controlli.

c) **Notifica delle violazioni di dati personali (artt. 33 e 34)**: in caso di violazione dei dati personali (perdita, distruzione o diffusione indebita, ovvero situazioni che possono comportare pericoli significativi per la privacy) il titolare del trattamento notifica la violazione all'Autorità Garante senza ritardo, e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che detta violazione presenti un rischio per i diritti e le libertà dell'interessato. A tale riguardo, l'Autorità Garante redigerà e renderà pubblico un elenco delle tipologie di trattamento soggette a tale obbligo.

d) **Valutazione d'impatto sulla protezione dei dati personali e designazione del responsabile della protezione dei dati (artt. 35 e 37):** quando un tipo di trattamento prevede l'uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà della persona fisica, il titolare è tenuto ad effettuare, prima di procedere, una valutazione d'impatto dei trattamenti previsti sulla protezione dei dati personali. Tra i nuovi adempimenti è prevista l'adozione di una nuova figura professionale obbligatoria, ossia il Responsabile per la protezione dei dati personali (DPO), comunque obbligatoria solamente nel caso di aziende dove i trattamenti presentino specifici rischi, nelle quali sia richiesto un monitoraggio regolare e sistematico degli interessati su larga scala, oppure che trattano dati sensibili. Dalla norma, si evince comunque che l'obbligo di designazione del DPO sussiste solo se il trattamento dei dati costituisce l'attività primaria e non meramente accessoria. Il responsabile può essere un dipendente del titolare oppure assolvere i suoi compiti in base ad un contratto di servizi e i suoi dati devono essere trasmessi all'autorità di controllo. Infine, detti responsabili dovranno essere muniti di competenze specifiche che, in assenza di una norma che ne stabilisca i contenuti, dovranno essere accertate dal titolare del trattamento prima del conferimento dell'incarico.

e) **Diritto all'oblio (art. 17):** l'interessato ha facoltà di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali non più necessari per le finalità per le quali sono stati raccolti ab origine, oppure nel caso di revoca del consenso, di opposizione al trattamento dei dati o quando il trattamento non sia conforme al Regolamento.

f) **Portabilità dei dati (art. 20):** l'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti ad un titolare del trattamento ed ha il diritto di trasmettere tali dati ad altro titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o questo sia necessario per l'esecuzione di un contratto.

g) **Diritto al risarcimento e responsabilità (art. 82)**: chiunque subisca un danno materiale o immateriale causato da una violazione di una norma del Regolamento (come recepita dalla legislazione nazionale) ha diritto di ottenere un risarcimento dal titolare, a meno che l'evento dannoso non sia imputabile a quest'ultimo.

h) **Sanzioni (artt. 83 e 84)**: ai sensi del Regolamento, l'Autorità Garante provvede affinchè le sanzioni amministrative pecuniarie siano in ogni singolo caso effettive, proporzionate e dissuasive. Il decreto di recepimento determinerà dette sanzioni nei limiti indicati dalla normativa comunitaria.

Gli uffici dell'Unione di Sondrio (dott. Mauro Romeri tel. 0342 533311) rimangono a completa disposizione per fornire ogni altra informazione o chiarimenti.