|  |  |  |  |
| --- | --- | --- | --- |
| ARGOMENTI | CATEGORIE | ADEMPIMENTI | RIFERIMENTI NORMATIVI |
| TRATTAMENTI DATI PERSONALI |  |  |  |
|  | * Dipendenti | * Informativa * Verifica categorie di dati trattati e finalità dei trattamenti * Durata conservazione dati * Consenso al trattamento dei dati, trattamento in esecuzione di un contratto, legittimo interesse del titolare | ART.13 GDPR  Opinion n. 2 dell’8.6.2017 del WP 29 |
|  | * Dipendenti - trattamento dati biometrici | * Informativa * Procedure di sicurezza per la conservazione dei dati biometrici * Selezione incaricati per accesso ai dati | ART.13 GDPR  Provvedimento Garante 12 novembre 2014 |
|  | * Dati dipendenti come dati di contatto (nei rapporti con clienti/fornitori) | * Utilizzo clausole contrattuali (o da inserire negli ordini, conferme d’ordine, e-mail, e più genericamente nelle comunicazioni con clienti/fornitori) | ART.13 GDPR |
|  | * Videosorveglianza | * Verifica rispetto art.4 St. lav. * Aggiornamento informativa privacy * Verifica procedure di conservazione dei dati * Verifica atto di nomina responsabile esterno ed eventuale aggiornamento * Verifica designazione incaricati | Provvedimento Garante 8 aprile 2010  Art.4 Statuto lavoratori  ART.28 GDPR  ART. 32, 4° comma, GDPR |
|  | * Geo-localizzazione autoveicoli   (altri strumenti elettronici) | * Verifica rispetto art.4 St. lav. * Aggiornamento informativa privacy * Verifica procedure di conservazione dei dati * Verifica atto di nomina responsabile esterno ed eventuale aggiornamento * Verifica designazione incaricati | Provvedimento Garante 4 ottobre 2011  Art.4 Statuto lavoratori  ART.28 GDPR  ARTT.29 e 32, 4° comma, GDPR |
|  | * Marketing | * Aggiornamento informative * Verifica procedure consenso * Conservazione dati e procedura revoca consenso | ARTT.13 e 14 GDPR  ARTT.130 e segg. Codice privacy  Provvedimento Garante 4 luglio 2013 |
|  | * Fidelity card | * Aggiornamento informative * Verifica procedure consenso * Conservazione dati e procedura revoca consenso | ART.13 GDPR  Provvedimento Garante 24 febbraio 2005 |
|  | * Gestione curricula | * Adeguamento informativa | ARTT.13 e 14 GDPR |
|  | * Policy privacy sito web | * Adeguamento policy * Verifica raccolta di dati attraverso il sito * Verifica profilazione utenti * Policy cookies | ARTT.13 e 14 GDPR  Provvedimento Garante 8 maggio 2014 |
|  | * E-commerce | * Informativa * Procedura consenso (se trattamenti anche per finalità di marketing e conservazioni consenso) | ART.13 GDPR |
| INDIVIDUAZIONE CATEGORIE DI ALTRI DATI TRATTATI |  |  |  |
|  | * Dati personali famigliari dipendenti * Consumatori/utilizzatori finali di prodotti/servizi aziendali * Ospiti aziendali | * Adeguamento informative * Verifica procedura accoglienza | ARTT.13 e 14 GDPR  Provvedimento Garante 8 aprile 2010 |
| ORGANIZZAZIONE INTERNA AZIENDALE |  |  |  |
|  | * Incaricati del trattamento | * Designazione incaricati ed istruzioni * Formazione incaricati | ARTT.29 e 32, 4° comma, GDPR |
|  | * Amministratori di sistema | * Adeguamento atti di nomina | Provvedimento Garante 27 novembre 2008 |
|  | * Responsabile interno privacy | * Delega di funzioni   *oppure*   * Mansionario |  |
|  | * Responsabili esterni al trattamento dati | * Verifica atto di nomina (distinto in ragione delle categorie di responsabili, es. software house, consulenti lavoro, società vigilanza, per attività geo-localizzazione, etc.) | ART.28 GDPR |
|  | * DPO | * Verifica presupposti di legge per nomina * Verifica requisiti candidati * Atto di nomina | ART.37 GDPR | Viene nominato ogniqualvolta:  a) il trattamento è effettuato da un'**autorità pubblica** o da un **organismo pubblico**, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;  b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il **monitoraggio regolare e sistematico degli interessati su larga scala**;  c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, **su larga scala**, di **categorie particolari di dati personali** di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'art.10. |
|  | * Nomina dell’azienda a responsabile esterno | * Verifica atto di nomina * Verifica adempimenti conseguenti (conformità all’atto di nomina) * Registro dei trattamenti del responsabile (*eventuale*) | ART. 28 GDPR  ART. 30 GDPR |
|  | * Sicurezza: misure tecniche e organizzative | (per tutte: “se del caso” = tenendo conto dei rischi e del contesto)   * Pseudonimizzazione e/o cifratura dei dati * Resilienza dei sistemi e dei servizi (software e app) * Strumenti e procedure di ripristino, per assicurare la disponibilità e l’accesso dei dati in caso di data breach * Procedura/e di verifica di efficacia e di riesame delle misure tecniche e organizzative * Istruzioni agli amministratori di sistema ed agli incaricati | ART. 32 GDPR |
| CONTITOLARITÀ |  |  |  |
|  | * Contitolarità infragruppo | * Individuazione trattamenti in contitolarità * Accordo di contitolarità | ART. 26 GDPR |
|  | * Contitolarità non infragruppo | * Individuazione trattamenti in contitolarità * Accordo di contitolarità | ART. 26 GDPR |
| DOCUMENTI MAPPATURE TRATTAMENTI |  |  |  |
|  | * Valutazione d’impatto trattamenti da compiere | * Verifica presupposti di legge * Adozione procedure di autovalutazione dei rischi * Riscontro documentale | ART.35 GDPR  Linee guida del WP 29 del 4.4.2017 | Richiesta, in particolare, nei seguenti **casi**:  a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;  b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'art.10;  c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. |
|  | * Registro dei trattamenti | * Verifica presupposti di legge * Redazione registro * Procedure di aggiornamento del registro | ART.30 GDPR | **Esclusioni**: imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'art. 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'art.10. |
|  | * Regolamento informatico | * Verifica rispetto art.4 St. lav. * Aggiornamento policy ed informativa dipendenti (inserimento obbligo di rispetto del Regolamento in lettera di assunzione) * Verifica designazione incaricati | Provvedimento Garante 1° marzo 2007  Art.4 Statuto lavoratori |
|  | * Data breach | * Procedure * Riscontro documentale | ARTT.33 e 34 GDPR |
|  | * Adozione codici di condotta settoriali e/o certificazione compiuta da organismi autorizzati | * Implementazione delle procedure | ARTT.40 e segg. GDPR |
|  | * Trasferimento dati all’estero | * Valutazione dei presupposti di liceità (decisioni di adeguatezza, garanzie adeguate e deroghe) | ARTT.44 e segg. GDPR |

GDPR = REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

WP 29 = GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Statuto dei lavoratori = Legge 20/05/1970 n. 300