



17/IT

WP 248 rev.01

**Linee guida in materia di valutazione d'impatto sulla protezione dei dati e
determinazione della possibilità che il trattamento "possa presentare un rischio elevato"
ai fini del regolamento (UE) 2016/679**

adottate il 4 aprile 2017

come modificate e adottate da ultimo il 4 ottobre 2017

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio MO-59 02/13.

Sito web: http://ec.europa.eu/justice/data-protection/index_en.htm

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ☐ una descrizione sistematica del trattamento è fornita (articolo 35, paragrafo 7, lettera a)):
 - ☐ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
 - ☐ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
 - ☐ viene fornita una descrizione funzionale del trattamento;
 - ☐ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);
 - ☐ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);
- ☐ la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):
 - ☐ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
 - ☐ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
 - ☐ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
 - ☐ liceità del trattamento (articolo 6);
 - ☐ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
 - ☐ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
 - ☐ misure che contribuiscono ai diritti degli interessati:
 - ☐ informazioni fornite all'interessato (articoli 12, 13 e 14);
 - ☐ diritto di accesso e portabilità dei dati (articoli 15 e 20);
 - ☐ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
 - ☐ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
 - ☐ rapporti con i responsabili del trattamento (articolo 28);
 - ☐ garanzie riguardanti trattamenti internazionali (capo V);
 - ☐ consultazione preventiva (articolo 36).
- ☐ i rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):
 - ☐ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
 - ☐ si considerano le fonti di rischio (considerando 90);
 - ☐ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
 - ☐ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
 - ☐ sono stimate la probabilità e la gravità (considerando 90);
 - ☐ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);
- ☐ le parti interessate sono coinvolte:
 - ☐ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
 - ☐ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).