Il **Regolamento (UE) 2016/679 - GDPR** impone al titolare del trattamento dei dati, di adottare "**misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**" (art. 24, par. 1). Tale obbligo si inserisce nel principio generale di **accountability** (art. 5, par. 2), che richiede di rendere effettiva e dimostrabile la responsabilità del titolare nell'assicurare la protezione dei dati personali. In particolare, l'art. 32 richiede di assicurare un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché della probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche.

In coerenza con il principio di **protezione dei dati by design e by default** (art. 25), il titolare è tenuto a integrare soluzioni idonee a ridurre i rischi di accesso non autorizzato.
Il **Considerando 83** precisa che, per prevenire trattamenti illeciti o non conformi, il titolare o il responsabile devono valutare i rischi inerenti al trattamento e attuare misure adeguate, come la cifratura, l'autenticazione e la minimizzazione dei dati. Tra queste, l'**autenticazione a più fattori (MFA)** rappresenta una misura adeguata e proporzionata, espressamente riconducibile all'obbligo di rafforzare i meccanismi di sicurezza per la salvaguardia dei dati e delle informazioni. La sua implementazione costituisce pertanto, per il Ministero, un adempimento necessario ai fini della conformità al GDPR.

Il GDPR pone quindi già oggi l'obbligo di adottare misure di sicurezza cibernetica adeguate alla protezione dei dati personali; in continuità con esso si colloca la Direttiva NIS2, che rafforza questi obblighi e specifica in modo esplicito alcune misure, come l'autenticazione a più fattori, già considerate adeguate dal Regolamento europeo.

Il **DECRETO LEGISLATIVO 4 settembre 2024, n. 138**, che recepisce la direttiva (UE) 2022/2555 (NIS2), relativa alle misure per garantire un livello comune elevato di cibersicurezza nell'Unione Europea, stabilisce, all'art. 24 (Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica), che i soggetti essenziali e i soggetti importanti debbano adottare misure adeguate alla gestione dei rischi per la sicurezza dei sistemi informativi e di rete.

In particolare, al punto l) dell'articolo in questione, è previsto che tali soggetti debbano implementare soluzioni di autenticazione a più fattori o di autenticazione continua, oltre a comunicazioni vocali, video e testuali protette, nonché sistemi di comunicazione di emergenza protetti, qualora ciò risulti opportuno per la sicurezza interna dell'organizzazione.

Di seguito si riporta il link alla gazzetta ufficiale dove è possibile consultare il testo integrale ed originale del DL Gazzetta Ufficiale

Il quadro normativo nazionale già da tempo evidenzia la necessità di adottare sistemi di autenticazione robusti per la protezione dei sistemi informativi della pubblica amministrazione. In particolare, il Codice dell'Amministrazione Digitale (d.lgs. 82/2005), all'art. 64, disciplina l'utilizzo di sistemi di identità digitale come SPID, che prevedono livelli avanzati di autenticazione; gli artt. 50–51 richiedono misure atte a garantire integrità, riservatezza e continuità operativa.

Le Linee guida AgID, adottate ai sensi dell'art. 71 CAD con parere del Garante Privacy, ribadiscono l'esigenza di meccanismi di autenticazione forte nei sistemi della PA. Lo stesso Garante, già dal 2013, ha indicato forme di "autenticazione forte" come misura di sicurezza idonea, e in recenti provvedimenti ispettivi ha sottolineato l'importanza dell'MFA in particolare per accessi remoti e infrastrutture critiche.

Il **Codice dell'Amministrazione Digitale (d.lgs. 82/2005)**, pone le basi per l'utilizzo di sistemi di autenticazione avanzata: l'art. 64 disciplina SPID, basato su livelli di autenticazione forte; gli artt. 50 e 51 richiedono misure idonee a garantire integrità, riservatezza e disponibilità dei sistemi; l'art. 71 prevede che le Linee guida AgID siano sottoposte al parere del Garante Privacy, assicurando coerenza con la protezione dei dati.

Le **Linee guida AgID sulla sicurezza ICT**, insieme alle regole tecniche su **SPID**, promuovono configurazioni robuste e l'uso di meccanismi di autenticazione forte, che di fatto incorporano la logica multifattoriale.

Il **Garante Privacy** ha ribadito questo orientamento: già nel 2013 raccomandava l'uso di autenticazione forte (OTP, certificati digitali) e, più recentemente, con provvedimenti ispettivi 2024–2025, ha richiesto la MFA per accessi remoti e sistemi critici, in applicazione del principio del minimo privilegio.

Infine, le **Linee guida AgID sull'interoperabilità** e il **Piano triennale per l'informatica nella PA** sottolineano l'evoluzione verso sistemi di autenticazione sempre più sicuri, confermando la MFA come misura coerente con gli standard richiesti alla pubblica amministrazione.