ALLEGATO B - REQUISITI GDPR
DATA PROTECTION BY DESIGN E BY DEFAULT

ADP nel proprio documento di conformità ha adottato l'approccio metodologico a qualsiasi progetto, in base al quale deve essere valutata la protezione dei dati personali sin dalla progettazione. Per qualunque attività di trattamento, quindi, sia strutturale sia ancora concettuale, si deve considerare la protezione dei dati personali dal momento della sua progettazione e si devono prevedere soluzioni per la protezione dei dati personali.

ADP mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento; in particolare le misure tecniche e organizzative messe in atto hanno lo scopo di garantire che – per impostazione predefinita – i dati personali vengano trattati solo per le specifiche finalità del trattamento e solo da un numero di persone fisiche limitato al perseguimento di dette finalità.

Si riportano qui di seguito i seguito i requisiti ai quali il concorrente deve attenersi nella presentazione dell'offerta tecnica per tutti i sistemi che trattano dati personali che dovranno essere compliance a tali requisiti.

a. REQUISITI MANDATORI

- Regolamento Europeo 679/2016 (GDPR)
- D.Lgs. 196/2003 Codice della privacy
- Provvedimento Amministratore di Sistema
- Provvedimento Internet e Posta Elettronica
- Provvedimento trattamento dati lavoratori privati
- L. 190/2012 e s.m.i. in materia di anticorruzione
- D.Lgs. 33/2013 in materia di trasparenza
- D.Lgs. 96/2005 Codice della navigazione
- Reg. (EU) n. 139/2014.
- Reg. (EU) n. 3001/2008 e relativi Regolamenti e Decisioni riservate di Dettaglio.
- Programma Nazionale di Sicurezza per l'Aviazione Civile
- Circolari e normativa secondaria emessa da Enac

b. REQUISITI VOLONTARI

- ISO/IEC 27001:2013 - Sistemi di gestione della sicurezza delle informazioni
- ISO/IEC 29100:2011 - Privacy Framework
- ISO/IEC 29134:2017 - Guidelines for privacy impact assessment.
- ISO/IEC 29151:2017 - Code of practice for personally identifiable information protection.
- ISO 31000:2018 - Guidelines, provides principles, framework and a process for managing risk.
- ISO 31010:2009 - Risk assessment techniques.

- UNI ISO 19600:2016 - Sistemi di gestione della conformità (compliance) Linee guida

Di seguito i requisiti di conformità al GDPR da richiedere/implementare in un SW che tratta dati personali onde poter assicurare la conformità dei trattamenti al Regolamento Europeo 679/2016 - GDPR.

RIFER.	PRINCIPIO	CIRCOSTANZA	REQUISITO
R 5.1.a	Correttezza	Trattamento Palese	Il SW non deve trattare dati personali in modo occulto rispetto all'utilizzatore.
R 5.1.a	Correttezza	Accesso Remoto	Qualora il SW consenta ad un operatore remoto di prendere il controllo della macchina locale per finalità di assistenza, l'intervento deve essere esplicito rispetto all'utilizzatore e possibilmente deve essere attivato/disattivato da questo.
R 5.1.a	Trasparenza	Info dati trattati	Le categorie dei dati personali dell'utilizzatore trattati e le modalità di trattamento devono essere rese note all'utilizzatore.
R 5.1.a.	Trasparenza	Log	Qualora il SW consenta la tracciatura delle attività (log) dell'utilizzatore deve essere reso noto all'utilizzatore il quale deve essere informato anche delle categorie di dati che vengono registrate
R 5.1.a	Liceità		ATTIVITA' DEL TITOLARE
R 5.1.b	Limitazione della finalità		vedi controllo di accesso - profili
R 5.1.c	Minimizzazione dei dati	Configurazione al minimo	Il SW deve essere configurabile in modo da consentire di restringere il trattameno ai soli dati necessari al titolare.
R 5.1.d	Esattezza	Aggiornabilità	Il SW deve consentire di aggiornare i dati, quando necessario al titolare.
R 5.1.d	Esattezza	Esattezza	Ove possibile il SW dovrebbe consentire di incrociare controlli per la coerenza dei dati: p.es. se c'è codice fiscale possibilità di verificarne l'esattezza con i dati di nascita; meccanismi di controllo per verificare errori di digitazione.
R 5.1.e	Limitazione della conservazione	Cancellazione	Il SW deve consentire di cancellare i dati quando non più necessari.
R 5.1.e	Limitazione della conservazione	Avviso di Cancellazione	Sarebbe opportuno che prima di attivare la cancellazione vi sia un warning per evitare cancellazioni accidentali.
R 5.1.e	Limitazione della conservazione	Modalità di Cancellazione	Per effetto della cancellazione i dati non devono poter essere recuperabili.
R 5.1.e	Limitazione della conservazione	Cancellazione Programmata	Sarebbe utile che il titolare possa programmare la cancellazione di dati impostando la scadenza. Questa funzione deve tener conto della limitazione.
R 5.1.f	Integrità e riservatezza	Inalterabilità	Il SW dovrebbe permettere al titolare di definire i livelli di inalterabilità che ritiene necessari. P.es. bloccare i dati rispetto alla modifica dopo la loro pubblicazione.
R 5.1.f	Integrità e riservatezza	Riservatezza	Il SW deve consentire l'accesso ai dati attraverso una procedura di autenticazione abbinata ad una di autorizzazione.
R 6.1.a R 9.2.a	Consenso	Informazione	Il SW deve permettere all'utilizzatore di verificare lo stato del consenso quando questa è la base giuridica del trattamento.
R 7.1	Evidenza del consenso	Evidenza	Qualora il SW preveda l'acquisizione del consenso deve poterne dare evidenza nel tempo.
R 7.2	Forma del consenso	Forma	Se il SW prevede che il consenso dell'interessato sia prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

RIFER.	PRINCIPIO	CIRCOSTANZA	REQUISITO
R 7.3	Revoca del consenso	Revoca	Se il SW prevede l'acquisisizone del consenso, deve prevederne anche la revoca con la medesima forma e modo.
R 11	Anonimizzazione	Anonimizzzione	Il SW, nel momento in cui i dati non devono più essere conservati, deve permettere al titolare, in alternativa alla cancellazione, di poter renderli anonimi, eliminando gli identificativi in modo irrecuperabile ed in modo che non siano più collegabili ad altri elementi di identificazione.
R 13	Informativa	Offerta Informativa	Qualora il Sw acquisisica il consenso è necessario che permetta la presa conoscenza dell'informativa, prima del conenso e poi ogni volta che l'interessato lo ritenga necessario.
R 12	Modalità informativa	Accesso all'Informativa	Il SW deve consentire l'accesso all'informativa in modo semplice ed intuitivo. Ove richiesto deve permettere di offrire informative in lingue diverse.
R da 15 a 21	Diritti degli interessati	Esercizio dei diritti	Il SW dovrebbe permettere, ove possibile, all'interessato di esercitare in modo semplice ed intuitivo i diritti riconodciutigli dal GDPR.
R 15	Diritto di accesso	Riscontro	Il SW deve offrire al titolare le informazioni necessarie al riscontro con particolare riferimento all'esistenza di dati del richiedente e le informazioni previste da R 15.
R 16	Diritto di rettifica	Rettifica	Il SW deve permettere al titolare di rettificare i dati, ove l'interessato eserciti fondatamente il diritto di rettifica. Questo anche quando i dati sono stati bloccati, tracciando la modifica.
R 17	Diritto di Cancellazione	Cancellazione	Il SW, ove l'interessato eserciti fondatamente il diritto di cancellazione, deve permettere al titolare di cancellare. Questo anche quando i dati sono stati bloccati, tracciando la modifica.
R 17	Diritto di Cancellazione	Cancellazione	Nel caso in cui vi sia stata diffusione, il SW, nei limiti del possibile deve permettere al titolare di individuare i soggetti che hanno creato link o fatto copie dei dati da cancellare in modo di poter inviare loro l'avviso di cancellazione.
R 18	Diritto di limitazione	Limitazione	Il SW, ove l'interessato eserciti fondatamente il diritto di limitazione, deve permettere al titolare di limitare i dati sino alla cessazione delle cause di limitazione.
R 19	Comunicazioni di cui sopra	Comunicazione	Il SW, qualora abbia consentito all'interessato di esercitare i diritti di cui sopra, deve poter dare informazione allo stesso dell'avvenuto adempimento da parte del titolare.
R 20	Diritto di portabilità	Portabilità dei Dati	Il SW, ove l'interessato eserciti fondatamente il diritto di portabilità, deve permettere al titolare di fornire all'interessato in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano e, ove richiesto dall'interessato, la possibilità di trasmettere tali dati a un altro titolare del trattamento.
R 21	Diritto di opposizione	Opposizione	Il SW, ove l'interessato eserciti fondatamente il diritto di opposizione, deve permettere al titolare di bloccare il trattamento dei dati oggetto di opposizione.
R 22	Automazione	Dichiarazione	Qualora il SW preveda il trattamento automatizzato compresa la profilazione, che produca effetti giuridici che riguardano o che incida in modo analogo significativamente sulla persona dell'interessato, deve dichiararlo manifestamente ed espressamente al titolare in modo da consentirgli di adottare le misure adeguate al caso.
R 24	Tracciabilità attività di conformità	Dichiarazione	La Softwarehouse, deve mettere a disposizione del titolare un documento che attesti le funzionalità che permettono al titolare di rispettare il GDPR.

RIFER.	PRINCIPIO	CIRCOSTANZA	REQUISITO
R 25	Privacy by design e by default	Dichiarazione	La Softwarehouse, deve sviluppare i SW che prevedono trattamento di dati personali, considerando ab origine i requisiti di conformità al GDPR e mantenerli nel corso della vita del SW.
R 28.1	Idoneità del fornitore	Dichiarazione	La Softwarehouse deve mettere a disposizione del cliente tutte le informazioni e/o certificazioni utili a dimostrare l'idoneità del fornitore rispetto agli obblighi del GDPR.
R 32.1	Protezione dei dati	Requisiti di sicurezza	Il SW deve poter essere configurato in modo da consentire il rispetto dei requisiti di sicurezza richiesti dal titolare.
R 32.1	Protezione dei dati	File di log	Il Sw deve consentire di proteggere i dati di log in modo da garantirne l'integrità, la riservatezza e la disponibilità.
R 32.1	Protezione dei dati	Profili di accesso	L'accesso all'applicativo, alle sue funzionalità (specie quelle di consultazione, modifica e cancellazione), alla configurazione, deve essere profilabile secondo le possibili necessità del cliente.
R 32.1.a	Pseudonimizzazione	Segregazione	Ove richiesto il SW deve poter permettere la segeregazione dei dati identificativi, o viceversa, di dati critici, in relazione a specifiche attività di trattamento o specifiche categorie di utenti. P.es. in caso di dati particolari.
R 32.1.a	Cifratura	Cifratura	Ove richiesto il SW deve poter consentire l'archiviazione o l'esportazione cifrata di specifiche categorie di dati personali (p.es. quelli relativi alla salute).
R 32.1	Protezione dei dati	Backup	Il Sw deve prevedere la funzione di salvataggio dei dati programmabile secondo le esigenze del cliente.
R 32.1.c	Ripristino	Ripristino	Il SW deve avere una funzione di ripristino in caso di disastro.
R 32.1.d	Test	Test	La Softwarehouse, prima di distribuire il SW o suoi upgrade deve prima testarne le funzionalità, con specifico riferimento a quelle di conformità al fine di accertarne l'efficacia. Di tali test deve essere data comunicazione al cliente.
R 35	DPIA	DPIA	La Softwarehouse, ove ricorrano le circostanze previste dall'art. 35 GDPR, deve condurre una DPIA preliminare a beneficio del cliente.