Tribunale di Asti

DOCUMENTO SULLA PRIVACY 2024/2025
Decreto Legislativo 30 giugno 2003, n. 196
Decreto legislativo 10 agosto 2018 n. 101
Decreto Legislativo 18 maggio 2018, n. 51
Regolamento (UE) 2016/679, "GDPR"

Il presente documento si intende reso in osservanza all'art. 15 D.lgs. n. 51/2018 – che prevede in capo al Titolare ed al Responsabile del trattamento l'obbligo di adottare misure tecniche ed organizzative che garantiscano un livello di sicurezza adeguato al rischio di violazione dei dati – recepisce le misure di sicurezza previste dal disciplinare tecnico contenuto nell'Allegato B) del Codice, sostituisce, il Documento Programmatico sulla Sicurezza e si adegua al Decreto Legislativo 18 maggio 2018, n. 51.
La disciplina del trattamento di particolari categorie di dati (art. 9, par.2, lett. f, GDPR) e giudiziari (art.10 GDPR) diversi da quelli trattati per ragioni di giustizia, ai sensi dell'art. 45-bis del Codice, in attuazione degli artt. 6, paragrafo 2, nonché dell'articolo 23, paragrafo 1, è contenuta nel relativo Regolamento, cui si rinvia.

MISURE DI SICUREZZA RIGUARDANTI IL TRATTAMENTO DI DATI PERSONALI CON STRUMENTI ELETTRONICI (ART. 25,2 D.lgs. N.51/2018)

Elenco dei trattamenti dei dati personali

I trattamenti sono gestiti in maniera informatica tramite l'utilizzo degli applicativi preposti alle funzioni e alle mansioni indicate negli ordini di servizio vigenti (P.D. n. 1/2024; P.D. n. 2/2024).

Distribuzione dei compiti e delle responsabilità

Titolare del trattamento per i dati personali trattati nei procedimenti civili e penali è il ***Tribunale di Asti***, nella persona della Presidente Dott.ssa Ombretta Salvetti o sostituto pro tempore, quale legale rappresentante. Restando, diversamente, in capo al Ministero della Giustizia la titolarità del trattamento dei dati relativi all'attività amministrativa.
È designata **Responsabile del trattamento** dei dati, la Dirigente dott.ssa Ada Maria Gomez Serito o sostituto pro tempore.
È stata designata **Responsabile della protezione** dei dati a livello nazionale, la dott.ssa Irene Sandulli (D.M. del 19/7/2023).

Incaricati del trattamento dei dati archiviati nelle banche informatiche sono i magistrati e il personale amministrativo nei limiti delle funzioni e delle mansioni indicate nel progetto organizzativo e negli

ordini di servizio vigenti. Sono altresì incaricati del trattamento i tirocinanti, nei limiti delle attività indicate nel progetto formativo, nonché coloro che per incarichi loro affidati vengano a contatto con dati personali.

Sono stati nominati in qualità di **Amministratore dei servizi informatici** gli assistenti informatici assegnati al Presidio Cisia di Torino, i quali possono essere coadiuvati nei propri compiti dai tecnici di un eventuale Raggruppamento Temporaneo di Imprese (R.T.I.) che svolgono assistenza sistemistica presso questo ufficio.

Compiti del **Titolare del trattamento:** decide in ordine alle finalità alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Compiti del **Responsabile del trattamento**: è preposto al trattamento dei dati personali dal Titolare; provvede all'adozione e all'aggiornamento del Documento contenente le Misure di sicurezza e del relativo Manuale per la sicurezza ad uso degli incaricati al trattamento dei dati; provvede alla realizzazione di quanto indicato nelle misure tecniche ed organizzative adottate al fine di garantire un livello di sicurezza adeguato al rischio di violazione dei dati.

Compiti del **Responsabile della protezione dei dati**: come previsti dall'art. 30 D.lgs. n. 51/18 cit.

Compiti dell'**Amministratore dei servizi informatici**:
svolge materialmente, anche con l'ausilio degli altri tecnici informatici del Raggruppamento Temporaneo d'Imprese nell'ambito dei contratti in corso, le operazioni necessarie a garantire il funzionamento del sistema informatico, sotto la direzione del Responsabile del trattamento; svolge i compiti attribuiti nel presente documento.

Compiti dei **preposti alla custodia della parola chiave**:
attivano le nuove utenze e, contestualmente provvedono alla comunicazione del nome utente e password; verificano almeno una volta al mese l'elenco delle persone autorizzate ad accedere agli archivi informatici; mettono in atto tutte le indicazioni contenute nel presente documento relative alla gestione della parola chiave.

Compiti degli **incaricati del trattamento**:
sono autorizzati a compiere le operazioni di trattamento dal titolare o dal responsabile;
rispettano le disposizioni contenute nel presente, nel Manuale di comportamento, nonché nel Regolamento sul trattamento dei dati sensibili e giudiziari.

Compiti del **personale appartenente all'Area Tecnica**:
svolgono, nell'ambito dei contratti in corso e in ausilio all'amministratore dei servizi informatici, le operazioni necessarie a garantire il funzionamento del sistema informatico.
Allo stato è in vigore un contratto per lo svolgimento di servizi di assistenza sistemistica ai server e alle postazioni di lavoro degli uffici giudiziari con le ditte facenti parte di un R.T.I.
I tecnici addetti sono designati quali incaricati del trattamento dei dati.

Sistema di autenticazione informatica

Tutti gli addetti possono accedere ai dati tramite specifiche credenziali di autenticazione per ogni trattamento dati al quale sono preposti.
Le postazioni di lavoro sono tutte migrate nell'Active Directory Nazionale (ADN), piattaforma nazionale unica sulla quale tutti gli utenti devono necessariamente autenticarsi per essere riconosciuti dal sistema e ottenere le necessarie credenziali per accedere ai servizi. Tale iniziativa, come indicato dalla Direzione Generale per i sistemi informativi automatizzati, volge a creare un ambiente lavorativo con alti requisiti di sicurezza, efficacia ed efficienza dei sistemi informativi presenti nell'Organizzazione della Giustizia. Ogni utenza per accedere nell'ADN è gestita in maniera autonoma da ogni ufficio attraverso i propri referenti alle consolle IAA e GSI, così da essere prontamente attivate le operazioni di trasferimento o di disabilitazione ogni qualvolta si verifichi tale necessità per via di trasferimento del personale e sua cessazione dal lavoro. Quindi è comprensibile come il sistema di autenticazione così progettato comporta questa prima procedura di accesso che riguarda il solo dominio giustizia e non anche le applicazioni, il quale accesso rimane regolato da profilature specifiche che prevedono un'ulteriore utenza e password, a disposizione del singolo utente che deve accedere alla determinata risorsa e dallo stesso custodita.

Active Directory Nazionale – Policy di Sicurezza ulteriori rispetto a quelle adottate a livello centrale

- nel gruppo di amministrazione delle PDL, per ogni Ufficio, viene inserito solo il personale tecnico strettamente necessario (scelto tra il personale CISIA e il personale dell'assistenza esterna contrattualizzata dal Ministero) escludendo gli amministratori centrali; accorgimento utile in concomitanza al monitoraggio ricorrente dei log;
- sono attivati i personal firewall delle PDL, questo accorgimento limita la possibilità di intrusione nelle PDL da parte di attaccanti presenti nella rete locale dell'Ufficio.

Analisi dei rischi- Misure di protezione

I rischi cui sono sottoposti i dati sono i rischi tipici di ogni sistema informatico e si distinguono in rischi legati ad eventi "fisici" quali guasti, sabotaggi, furti, intercettazioni, allagamenti o incendi, ed eventi legati a codice programma maliziosi, comunemente classificati come *virus, trojan horse, backdoor* o ancora da attività generata per rendere inutilizzabili i servizi di rete, tecnicamente nota come *"Denial of Service"*.
L'integrità fisica dei dati è affidata alle misure di sicurezza della sala server, il cui accesso, protetto da porta blindata, è consentito al personale del Presidio Cisia, ai tecnici informatici della ditta aggiudicataria della gara di assistenza sistemistica distrettuale, i quali si occupano anche della gestione delle copie automatiche giornaliere dei dati, che vengono prodotte ogni sera della settimana, ad eccezione dei giorni festivi e prefestivi.
La sala server è dotata di porta tagliafuoco, impianto antintrusione, condizionatore, che rendono lo stesso ambiente abbastanza sicuro da eventi "fisici" accidentali.
Tutti i server, nonché le singole postazioni di lavoro, sono protetti da antivirus attivo, indicato e fornito dal superiore Ministero, il cui compito è quello di proteggere i dati dai codice-programma "maliziosi", sopra indicati, e il cui aggiornamento viene effettuato in maniera automatica con frequenza giornaliera. Anche il sistema operativo di ogni singolo *pc* viene aggiornato in tempo quasi reale al rilascio da parte di Microsoft.
Inoltre, ogni *Server* è alimentato tramite un gruppo di continuità che filtra eventuali sbalzi di corrente e permette, in caso di assenza di elettricità, il corretto spegnimento del server, evitando quindi tutti i danni che possono verificarsi per gli sbalzi di tensione elettrica.

I server per la gestione della posta elettronica sono attualmente centralizzati presso enti indicati dal superiore Ministero, cui spetta l'onere di filtrare i messaggi contenenti codice "maligno".
Per quanto riguarda la protezione da eventuali attacchi *"Denial of Service"*, cioè mirati a rendere indisponibili i servizi di rete, si precisa che la rete di comunicazione dati è protetta da apposita apparecchiatura *Firewall*, configurata in remoto dall'apposito Centro di Sicurezza del Ministero, il cui compito è quello di evitare che utenti esterni alla rete possano accedere alle risorse interne al Palazzo di Giustizia di Asti
Pertanto, si ritiene che la rete sia protetta da attacchi esterni che possano portare al blocco di servizi di rete. L'attuale organizzazione dei sistemi informatici del ministero prevede che le basi dati e gli SW siano fisicamente dislocati in luoghi anche molto distanti dalla sede giudiziaria. In particolare, le basi dati e i sistemi del civile si trovano presso la sala CED di Roma mentre le basi dati e i sistemi del penale si trovano presso la sala CED distrettuale di Torino; per cui saranno tali strutture a garantire le politiche di sicurezza e di backup.

Criteri e modalità di ripristino in seguito a danneggiamento o distruzione - infrastruttura di backup

La gestione dei backup presso la sede di Asti è strutturata su due livelli, ciascuno con una specifica funzione e frequenza di esecuzione:

- **Primo livello - Backup locale (ogni 24 ore o meno)**
  Questo livello consiste nella copia dei dati all'interno dello stesso server che ospita il sistema principale. Di solito, questa operazione si traduce nella generazione di un *dump* di un *RDBMS* (*Relational Database Management System*, Sistema di Gestione di Database Relazionale), ovvero una copia completa dei dati e delle strutture del database per garantire un ripristino rapido in caso di perdita o corruzione di dati. La frequenza tipica di questo backup è ogni 24 ore, ma può essere configurata per intervalli più brevi in base alle esigenze operative e al volume dei dati trattati;
- **Secondo livello - Backup su server locale secondario (ogni 24 ore)**
  Il secondo livello prevede la copia dei dati, già salvati tramite il primo livello, su un server locale differente. Questo approccio fornisce una maggiore sicurezza, consentendo di preservare i dati anche in caso di guasto hardware o software sul server principale. I dati vengono trasferiti in modo sicuro e, in genere, con tecniche di compressione per ottimizzare lo spazio di archiviazione e la velocità del processo.

Primo livello	locale	ogni 24h o meno
Secondo livello	Secondo server locale	ogni 24h

Le tipologie di dati sottoposti a *backup* sono:

cartelle utenti/uffici (files di Office, cartelle generiche di scambio dati)	

Integrazione dei dispositivi NAS

Grazie all'acquisizione recente di dispositivi **NAS** (*Network Attached Storage*, Archiviazione Connessa alla Rete), è stato introdotto un ulteriore livello di protezione e ridondanza. I backup del primo e del secondo livello vengono replicati automaticamente su questi dispositivi. I NAS sono unità di archiviazione specializzate collegate alla rete locale (LAN), progettate per garantire accesso rapido, scalabilità e robustezza nella gestione dei dati.
L'utilizzo dei NAS offre vantaggi in termini di:

- *Ridondanza geografica locale*: Sebbene i dispositivi NAS siano fisicamente collocati nella stessa sede, permettono di distribuire i dati su dispositivi distinti, riducendo il rischio di perdita totale in caso di guasti multipli;
- *Accessibilità e velocità*: Grazie alla connessione diretta alla rete, i dati sono immediatamente disponibili per il ripristino, con prestazioni elevate rispetto ai backup tradizionali;
- *Scalabilità*: I NAS possono essere espansi facilmente per accogliere volumi crescenti di dati, senza interrompere le operazioni di backup.

Tipologia dei dati e frequenza di backup

Le tipologie di dati sottoposti a *backup* sono cartelle utenti/uffici (files di Office, cartelle generiche di scambio dati); esse sono, come già descritto, sottoposte a frequenza di backup giornaliera.

Scheduling

Le procedure di backup, insieme alle altre attività pianificate assieme alle procedure pianificate (indici REGE, copie particolari, altre attività), sono interamente gestite attraverso procedure batch[(1)]. Ogni server dispone di una procedura unica pianificata quotidianamente, che si occupa di eseguire tutte le attività previste per quel server. In alcuni casi, su determinati server, sono programmate più procedure batch, ma solo se queste seguono frequenze diverse, come una quotidiana e una settimanale.

Tutte le procedure batch sono centralizzate in un'unica cartella, ospitata sul server di backup, per facilitarne la gestione e la manutenzione. Le operazioni comuni, come la copia dei dati, il *logging*, la gestione degli indici *REGE* (*Registro Generale degli Affari Civili e Penali*) e i *dump*[(2)], sono suddivise in sotto-procedure batch modulari e parametrizzate, garantendo flessibilità e semplicità di aggiornamento.

Sebbene il sistema *REGE* non sia più utilizzato in produzione e sia ora destinato esclusivamente alla consultazione, per ragioni di sicurezza sono state conservate le originarie procedure di backup legate a questo sistema.

(1) Batch: una procedura batch è un insieme di istruzioni o comandi che vengono eseguiti automaticamente, senza l'intervento umano, solitamente in momenti pianificati. Questo approccio è utilizzato per eseguire compiti ripetitivi o complessi, come backup, generazione di indici o esportazione di dati, garantendo precisione e affidabilità.

(2) Dump: termine tecnico che indica una copia completa dei dati contenuti in un database, generalmente in formato leggibile o ripristinabile.

MISURE DI SICUREZZA RIGUARDANTI IL TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (ART. 25 D.lgs. N.51/2018)

Gli incaricati del trattamento dei dati gestiti con modalità cartacea sono i magistrati e il personale amministrativo nei limiti delle funzioni e delle mansioni indicate nel progetto tabellare e negli ordini di servizio vigenti. Sono altresì incaricati del trattamento i tirocinanti nei limiti delle attività indicate nel progetto formativo.

a) Sicurezza degli uffici e conservazione dei dati

Durante l'orario di lavoro, gli uffici sono presidiati dal personale incaricato. Al termine dell'orario lavorativo, il personale addetto chiude a chiave gli uffici, lasciando per ultimo il luogo di lavoro.
Gli studi dei magistrati sono custoditi dai magistrati stessi; in caso di assenza, gli studi vengono chiusi a chiave.
Atti e documenti contenenti dati sensibili o giudiziari, utilizzati per l'attività amministrativa e gestionale, sono conservati in armadi o schedari chiusi a chiave dal personale incaricato. Le cartelle cliniche, quando trattenute per esigenze amministrative, sono custodite in armadi blindati dotati di chiavi di sicurezza, custodite dal responsabile del trattamento.

b) Protezione dei dati personali da accessi estranei

Gli incarti contenenti dati personali non devono essere visibili o accessibili a soggetti estranei. Durante l'orario di apertura al pubblico, gli utenti sono invitati a mantenere una certa distanza da chi sta ricevendo informazioni o servizi. Accorgimenti come il capovolgimento degli incarti vengono adottati nel caso di avvicinamento di persone non coinvolte.
Nelle cancellerie sono presenti divisori che delimitano lo spazio accessibile al pubblico.
L'accesso del pubblico agli uffici è vietato.

c) Accesso agli archivi

I locali utilizzati come archivi non sono accessibili al pubblico. L'accesso è controllato e consentito solo a personale autorizzato dal funzionario capo settore.

d) Registro delle intercettazioni

Il registro delle intercettazioni contiene esclusivamente i seguenti dati:

- Numero delle notizie di reato;
- Numero delle utenze;
- Data di ricezione;
- Data del decreto del G.I.P. (Giudice per le Indagini Preliminari);
- Date delle eventuali proroghe e del deposito;
- Nome del giudice.

e) Rilascio di copie degli atti

Le copie degli atti possono essere rilasciate esclusivamente dal personale autorizzato.
Gli utenti, siano essi professionali (avvocati, consulenti) o non professionali, devono presentare una richiesta scritta specificando l'uso della copia. La richiesta può essere presentata personalmente o tramite un incaricato alla cancelleria competente.
Le copie sono rilasciate dall'ufficio entro i termini di legge e seguendo l'ordine di presentazione.

f) Accesso alle decisioni dell'autorità giudiziaria

Le decisioni dell'autorità giudiziaria sono consultabili, per finalità di informazione giuridica, dai rappresentanti di case editrici o riviste giuridiche, esclusivamente alla presenza di un addetto all'ufficio. Tale accesso deve sempre essere autorizzato dal capo dell'ufficio giudiziario.
Si richiamano le linee guida del Garante per la Protezione dei Dati Personali del 02/12/2010 sul trattamento dei dati personali nella riproduzione di provvedimenti giurisdizionali.

g) Dati personali nelle vendite giudiziarie

Negli avvisi di vendita, nelle copie delle ordinanze del giudice e nelle relazioni di stima, non devono essere indicati il nome del debitore né altri dati personali idonei a rivelarne l'identità.
Per rispettare il principio di proporzionalità nel trattamento dei dati, nelle copie pubblicate degli atti devono essere omessi i dati personali di soggetti estranei alla procedura esecutiva.

h) Trattamento dei dati da parte di consulenti tecnici e periti

I magistrati, al momento dell'assegnazione di incarichi, devono invitare consulenti tecnici e periti al rigoroso rispetto delle disposizioni stabilite dal Garante della privacy nella delibera n. 46 del 26/06/2008.

i) Informativa ai soggetti esterni

Ai soggetti esterni che comunicano dati personali per attività amministrative dell'Ufficio è fornita l'informativa prevista dall'art. 10 del D.Lgs. 51/08.

***

Si allegano:
- il "Manuale di sicurezza" che contiene le disposizioni specifiche impartite al personale per garantire la sicurezza dei dati trattati con strumenti elettronici;
- il Provvedimento Presidenziale del _____ con il quale si designano il Responsabile e gli incaricati al trattamento dei dati personali.

Asti, 11 DIC. 2024

In qualità di responsabile del trattamento
La Dirigente Amministrativa

in qualità di titolare del trattamento
La Presidente del Tribunale