

Ispezioni e Garante

Csi Piemonte

Torino, 16 febbraio 2023 Mauro Alovisio

# Presentiamoci: Chi siamo



Mauro Alovio

Avvocato presso Università, mi occupo da diversi anni di protezione dati e del diritto delle nuove tecnologie, **coordinatore del primo corso di perfezionamento universitario in materia di protezione dei dati personali** dell'Università degli Studi di Torino (Direttore: Prof. Francesco Pizzetti e prof. Sergio Foà), componente del Comitato Etico Città della salute

**professore a contratto** presso l'Università Statale di Milano, docente presso master di cybercrime dell'Università degli Studi di Torino, presidente del Centro Studi di informatica Giuridica di Ivrea Torino, Fellow del Centro di ricerca Nexa su Internet e società del Politecnico di Torino. Formatore e autore di pubblicazioni



# Dipartimento di Giurisprudenza

## Corsi di Studio del Dipartimento di Giurisprudenza

- Home
- I corsi ▾
- Iscriversi ▾
- Studiare ▾
- Laurearsi ▾
- English ▾

Home / Data protection officer



Pagina in aggiornamento

**Quarta edizione del corso di perfezionamento in diritto della protezione dei dati personali per la formazione del data protection officer (DPO) profili applicativi**



fondo  
sociale europeo



# MASTER IN INNOVAZIONE DIGITALE E LEGAL COMPLIANCE



GESTITO DA  
**COREP**

IN COLLABORAZIONE CON  
**Skillab**

UNIVERSITÀ DEGLI STUDI DI TORINO  
 MASTER DI I LIVELLO IN INNOVAZIONE DIGITALE E LEGAL  
 COMPLIANCE  
 II EDIZIONE A.A. 2022/23

## NEWS

SCADENZA ISCRIZIONI: 15 MARZO 2023  
 SI INVITANO I CANDIDATI INTERESSATI AD INVIARE AL PIÙ PRESTO IL  
 PROPRIO CURRICULUM E LA DOMANDA DI ISCRIZIONE (VEDI SEZIONE  
 ISCRIZIONI E SCADENZE)

LE SELEZIONI SARANNO EFFETTUATE SECONDO L'ORDINE DI ARRIVO DELLE  
 CANDIDATURE

Il Master in Innovazione Digitale e Legal Compliance, proposto in modalità  
 apprendistato, è un Master di I livello dell'Università degli Studi di Torino della durata di  
 due anni con assunzione effettuata dalle aziende aderenti fin dall'inizio del master.

Il master si propone di dare una formazione specialistica per la creazione di figure  
 professionali da inserire in quei settori aziendali che hanno nel loro modello di sviluppo  
 la transizione verso il digitale e che, tramite l'implementazione di tecnologie  
 abilitanti, perseguono strategie data driven di smart industry.

Il Master è attivato dal Dipartimento di Giurisprudenza (capofila) e dal  
 Dipartimento di Informatica dell'Università degli Studi di Torino.

Il Master è realizzato in collaborazione con l'Unione Industriale di Torino e con  
 Confooperative Piemonte.

# HAI MENO DI 29 ANNI E SEI LAUREATO?

**11 imprese piemontesi assumono con  
contratto in alto apprendistato**

## Perché candidarsi?

- MASTER DI 2 ANNI GRATUITO
- ASSUNZIONE IN AZIENDA PIEMONTESE

## Cosa imparerai?

PRIVACY E DATA PROTECTION, INFORMATICA E  
CYBERCRIME, BIG DATA, IOT E INTELLIGENZA ARTIFICIALE,  
ETICA E PARI OPPORTUNITÀ, DIRITTO AZIENDALE

**SCADENZA CANDIDATURE: 15 MARZO 2023**



**MASTER IN INNOVAZIONE DIGITALE  
E LEGAL COMPLIANCE**

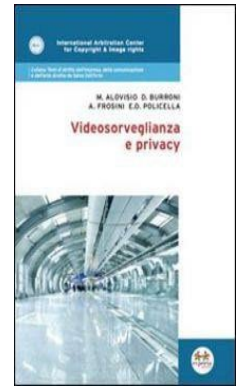
MASTER  **LEGAL  
INNOVATION**

**Per candidarsi:**

**[www.masterlegalinnovation.it/  
iscrizioni/iscrizioni-e-scadenze.html](http://www.masterlegalinnovation.it/iscrizioni/iscrizioni-e-scadenze.html)**



# Centro Studi di Informatica Giuridica di Ivrea Torino



Il Centro Studi di Informatica Giuridica di Ivrea-Torino (CSIG) è un'associazione indipendente senza finalità di lucro attiva dal 2005 interdisciplinare (rivolta a giuristi, informatici, etc.)

Mission: aggiornamento professionale, studio, approfondimento dell'evoluzione dei diritti digitali, dell'ICT e dell'Informatica Giuridica a livello locale e nazionale

Aderisce alla rete nazionale alla relativa mailing list (900 professionisti)

A livello piemontese: ha due sedi una storica a Ivrea e una a Torino, un blog <http://csigivreatorino.it> ed un Comitato Scientifico di magistrati, professori e avvocati.

Ha partecipato alle consultazioni on line in materia di trasparenza, open data. software libero, wi-fi, cyberbullismo, etc..

---

# AGENDA

- ✓ *Ispezioni*
- ✓ Videosorveglianza
  - ✓ DPIA
- ✓ Whistleblowing
  - ✓ App

## Finalità delle ispezioni

- ✓ Strumento di garanzia dei cittadini e imprese
- ✓ Strumento di governo del sistema in un'ottica non solo repressiva ma anche conoscitiva
- ✓ Strumento di prevenzione





## AMMINISTRATIVO



PRIVACY | 01 Aprile 2021

## Protocollo di intesa tra Guardia di Finanza e Garante Privacy: una nuova stagione dei controlli e ispezioni

di Mauro Alovio - Avvocato

Il Garante, alla luce dell'evoluzione del quadro normativo europeo e nazionale e delle innovazioni tecnologiche e di comunicazione, rafforza la sinergia con la Guardia di Finanza, nell'ottica anche di una più intensa collaborazione anche in ambito ispettivo tra le varie Autorità di controllo, operanti in ambito europeo e internazionale.



La Guardia di Finanza e il Garante per la protezione dei dati personali hanno rinnovato in data 31 marzo 2021 il **protocollo di intesa** fra le due istituzioni.

Il nuovo accordo ha la finalità di rafforzare le preziose **sinergie** in essere finalizzate al miglioramento dell'efficacia complessiva delle attività connesse alla vigilanza sul rispetto delle norme che disciplinano la tutela dei dati personali.

La collaborazione fra Garante e Guardia di Finanza era stata oggetto di precedenti protocolli di intesa, sottoscritti il 26 settembre 2002, l'11 novembre 2005 e il 10 marzo 2016: il codice della privacy prevede, infatti, la possibilità che il personale del Garante possa essere assistito, nell'esecuzione degli accertamenti, da altri organi dello Stato (art. 158, comma 3, del codice).

## Notizie correlate

La cartella sanitaria inviata alla persona sbagliata rappresenta un data breach importante

Per chi rientra in Italia dopo aver soggiornato all'estero quarantena di 5 giorni e test molecolare

Assistenti vocali, immagini di persone in manette e permessi per l'accesso in ZTL: la parola al Garante Privacy

Il Presidente del Consiglio deve riesaminare le misure adottate per la DAD in zona rossa

Tra avvocati italiani e stabiliti non vi è disparità di trattamento ai fini dell'accesso all'albo cassazionisti

# AGENDA

- ✓ Ispezioni
- ✓ *Videosorveglianza*
  - ✓ DPIA
- ✓ Whistleblowing
  - ✓ App

## Videosorveglianza: caso concreto

- ✓ Struttura e organizzazione dell'ente
  - ✓ Titolarità del trattamento
  - ✓ Descrizione delle finalità
  - ✓ Tipologie di dati trattati
- ✓ Accesso e visione delle immagini , verifica della qualità delle immagini, accesso da remoto all'impianto, impostazioni
  - ✓ Cancellazione delle immagini
- ✓ Il Garante invita a comprovare con idonea documentazione le scelte dell'ente e il rispetto dei principi del trattamento

## Videosorveglianza e comuni

- ✓ Descrizione della funzionalità delle telecamere con relativa documentazione
  - ✓ Data di installazione delle telecamere
- ✓ Numero di telecamere dotate , mappa del territorio con indicazione dei siti
  - ✓ Finalità di trattamento e la base giuridica
  - ✓ Copia eventuale patto per la sicurezza urbana
- ✓ Copia della valutazione di impatto e il parere del DPO

# AGENDA

- ✓ Ispezioni
- ✓ Videosorveglianza
  - ✓ *DPIA*
- ✓ Whistleblowing
  - ✓ App



# GPDP

GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Inserire il testo o il doc web

CERCA



I miei diritti



Imprese ed enti

L'Autorità

Temi

Normativa e provvedimenti

News e comunicazione

Amministrazione trasparente

Home / Stampa e comunicazione / Comunicato stampa

/ Lavoro: il Garante privacy sanziona la Regione Lazio. Illecito controllo di metadati delle e-mail di dipendenti

## Lavoro: il Garante privacy sanziona la Regione Lazio. Illecito controllo di metadati delle e-mail di dipendenti



**Lavoro: il Garante privacy sanziona la Regione Lazio**  
**Illecito controllo di metadati delle e-mail di dipendenti**

No al controllo dei metadati della posta elettronica dei dipendenti senza adeguate tutele per la riservatezza e in violazione delle norme che limitano il controllo a distanza dei lavoratori.

Questa la decisione del Garante per la privacy nei confronti della Regione Lazio, cui ha comminato una **sanzione di 100.000 euro** e vietato i trattamenti tuttora in corso.

Il caso nasce dalla segnalazione di un sindacato che aveva lamentato un

### Scheda

Doc-Web  
9833616

Data  
19/12/22

### Argomenti

Informativa e-mail

Lavoro dipendente Lavoro pubblico

DPIA

### Tipologie

Comunicato stampa



# GPDP

**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

Inserire il testo o il doc web

**CERCA**



I miei diritti



Imprese ed enti

[L'Autorità](#) ▾ [Temi](#) ▾ [Normativa e provvedimenti](#) ▾ [News e comunicazione](#) ▾ [Amministrazione trasparente](#)

[Home](#) / [Provvedimenti](#) / [Ordinanza ingiunzione o revoca](#)

/ [Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021 \[9703988\]](#)

## Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi Bocconi" di Milano - 16 settembre 2021 [9703988]



[doc. web n. 9703988]

**Ordinanza ingiunzione nei confronti di Università Commerciale "Luigi  
Bocconi" di Milano - 16 settembre 2021**

Registro dei provvedimenti  
n. 317 del 16 settembre 2021

**IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI**

### Scheda

Doc-Web  
9703988

Data  
16/09/21

### Argomenti

Biometria

Trasferimento dati all'estero

Università

Profilazione

### Tipologie

Ordinanza ingiunzione o revoca

## Valutazione di impatto privacy (a)

✓ Le recenti sanzioni del Garante privacy hanno rilevato, ad esempio, l'assenza in diversi casi di una valutazione di impatto privacy prevista dall'art. 35 del GDPR, valutazione che risulta obbligatoria ai sensi delle indicazioni delle Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248) in presenza di due fattori, spesso concomitanti, in ambito sanitario: quali: il trattamento di **“dati sensibili o aventi carattere altamente personale”** e di **“dati relativi ad interessati vulnerabili”**.

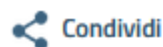
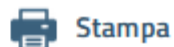


## Valutazione di impatto privacy (b)

✓ “Si ritiene, poi, che, con riferimento al caso di specie, possano essere soddisfatti anche i criteri relativi al “trattamento di dati su larga scala” considerato che, secondo quanto dichiarato dall’Azienda il trattamento ha riguardato oltre 13.500 e **l’uso innovativo o l’applicazione di nuove soluzioni tecnologiche od organizzative** (cfr. richiamate Linee guida, III, lett. B, punti 5 e 8).

[Home](#) / [Provvedimenti](#) / [Ammonimento](#) / [Provvedimento del 13 maggio 2021 \[9687977\]](#)

# Provvedimento del 13 maggio 2021 [9687977]



[doc. web n. 9687977]

## Provvedimento del 13 maggio 2021


Registro dei provvedimenti  
n. 201 del 13 maggio 2021

### IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

## Scheda

 Doc-Web  
9687977

 Data  
13/05/21

## Argomenti

Sanità e ricerca scientifica

Dati sanitari

Pazienti

App

## Tipologie

Ammonimento

in particolare che:

- pur rientrando la fattispecie in esame tra quelle per le quali il titolare è tenuto ad effettuare, "prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali" (art. 35 del Regolamento), in considerazione della natura dei dati trattati (dati relativi alla salute) su larga scala, della categoria di soggetti vulnerabili degli interessati e che il trattamento è effettuato attraverso l'applicazione di nuove soluzioni tecnologiche, la valutazione di impatto effettuata dall'Azienda, come indicato nella citata nota del 25 giugno 2020, risultava priva di alcuni degli elementi indispensabili richiesti dall'art. 35, par. 7 del Regolamento e, in particolare, di una valutazione circa la necessità e la proporzionalità dei trattamenti in relazione alle finalità perseguite, dell'indicazione degli specifici rischi per i diritti e le libertà degli interessati che il trattamento in oggetto potrebbe comportare, considerato che alcuni dei rischi indicati nella valutazione trasmessa risultavano del tutto inconferenti, rispetto alle caratteristiche dell'applicazione attraverso la quale il trattamento era effettuato (es. "Mal di testa transitorio") e delle misure adottate per affrontare i rischi, considerato che non è stata descritta nessuna misura in tal senso, né di carattere tecnico, né organizzativo. Ulteriori elementi di criticità della predetta valutazione riguardavano il rispetto del principio di minimizzazione dei dati e quello di limitazione della conservazione, nonché, come sopra indicato, l'incoerenza del contenuto rispetto a quanto sostenuto in altri documenti aziendali trasmessi all'Autorità;

- le informazioni rese agli interessati, ai sensi dell'art. 13 del Regolamento, attraverso il modello denominato "Trattamento dei dati sanitari presso il

# AGENDA

- ✓ Ispezioni
- ✓ Videosorveglianza
  - ✓ DPIA
- ✓ *Whistleblowing*
  - ✓ App

Health Media Company  
 SCRIVEREMO IL TUO FUTURO


Società Italiana di Comunicazione Scientifica e Sanitaria


**RICERCHIAMO UN SUPERVISORE  
 DI LABORATORI DI RICERCA**

 VISITA IL NOSTRO  
 SITO PER SAPERNE  
 DI PIU!

 segui [quotidianosanità.it](#)


twitter



facebook



feed



newsletter



archivio

[Tweet](#) | [Condividi](#) | [Condividi 4](#) | [stampa](#)

## Whistleblowing senza privacy: Garante sanziona ospedale Perugia e società informatica

**L'accesso all'applicazione web di whistleblowing, basata su un software open source, avveniva attraverso sistemi che, non essendo stati correttamente configurati, registravano e conservano i dati di navigazione degli utenti, tanto da consentire l'identificazione di chi la utilizzava, tra cui i potenziali segnalanti**

**12 MAG** - PA e imprese devono prestare la massima attenzione nell'impostazione e gestione dei sistemi di whistleblowing, garantendo la massima riservatezza dei dipendenti e delle altre persone che presentano segnalazioni di condotte illecite. Lo ha ribadito il Garante per la privacy che [ha sanzionato azienda ospedaliera di Perugia e la società informatica](#) che gestiva il servizio per denunciare presunte attività corruttive o altri comportamenti illeciti all'interno dell'ente.

L'istruttoria dell'Autorità nasce nell'ambito di un ciclo di attività ispettive sulle modalità di trattamento dei dati acquisiti tramite i sistemi di whistleblowing, in particolare quelli più utilizzati in Italia dai datori di lavoro.

Dai controlli effettuati presso un'azienda ospedaliera sono emerse diverse violazioni del Gdpr. L'accesso all'applicazione web di whistleblowing, basata su un software open source, avveniva attraverso sistemi che, non essendo stati correttamente configurati, registravano e conservano i dati di navigazione degli utenti, tanto da consentire l'identificazione di chi la utilizzava, tra cui i potenziali segnalanti.

La struttura sanitaria non aveva poi provveduto a informare preventivamente i lavoratori in merito al trattamento dei dati personali effettuato per finalità di segnalazione degli illeciti, non aveva effettuato una valutazione di impatto privacy e non aveva neppure inserito tali operazioni nel registro delle attività di trattamento, strumento utile per valutare i rischi per i diritti e le libertà degli interessati. È infine emersa una non corretta gestione delle credenziali di autenticazione per l'accesso all'applicazione web di whistleblowing da parte del Responsabile della prevenzione della corruzione e della trasparenza (Rpct), durante la fase di transizione con il suo successore.

Nel corso dei controlli sono emersi ulteriori illeciti imputabili alla società informatica che, in qualità di responsabile del trattamento, forniva all'azienda ospedaliera l'applicazione web di whistleblowing. La società si era infatti avvalsa di un fornitore esterno per il servizio di hosting dei sistemi che ospitavano l'applicativo senza dare specifiche istruzioni sul trattamento dei dati degli interessati e senza darne notizia alla struttura sanitaria. Aveva poi utilizzato il medesimo servizio di hosting anche per proprie finalità, ad esempio per la gestione del rapporto di lavoro con i dipendenti o la gestione contabile e amministrativa, anche in questo caso senza regolare il rapporto e fuso dei dati.

Il Garante, tenendo conto della piena collaborazione offerta nel corso dell'istruttoria anche per sanare i problemi rilevati, ha comminato sia alla struttura sanitaria sia alla società informatica una sanzione di 40.000 euro. Ha inoltre concesso 30 giorni alla società informatica per adeguare il rapporto con il fornitore del servizio di hosting alla normativa sulla protezione dei dati personali.

**È uscito**  
**il fascicolo**  
**N10 DICEMBRE**  
 di  
**TOSCANA**  
**MEDICA**

**10**

[DOWNLOAD PDF](#)

**OSnewsletter**
[ISCRIVITI ALLA NOSTRA NEWS LETTER](#)

 Ogni giorno sulla tua mail tutte le notizie di  
 Quotidiano Sanità.

**THE LIFESCIENCE EXCELLENCE SHOW**

[GUARDA IL PROGRAMMA](#)

**OS gli speciali**

**Approvata la prima legge di  
 Bilancio del Governo  
 Meloni. Fondo sanitario  
 sale a 128,211 miliardi.**
**Ecco tutte le misure per la  
 sanità**

# Whistleblowing

- ✓ informazioni trasparenti e chiare
- ✓ accordo a responsabile esterno
- ✓ scheda aggiornata del registro dei trattamenti come responsabili
  - ✓ valutazione di impatto privacy
- ✓ adozione misure di sicurezza accesso piattaforma

# AGENDA

- ✓ Ispezioni
- ✓ Videosorveglianza
  - ✓ DPIA
- ✓ Whistleblowing
  - ✓ *App*

# Un mondo di app

- un'informativa completa sui trattamenti resi possibili dall'applicativo.
- Assenza di accordo a responsabile esterno rapporto con la società fornitrice del sistema di prenotazione.
  - le misure tecniche e organizzative implementate dall'Ente,
- Violazione dell'art. 4 dello Statuto dei lavoratori in relazione alla funzione che consente di produrre report sull'attività degli addetti allo sportello, introdotta senza le necessarie garanzie previste dallo Statuto dei lavoratori sul controllo a distanza.
  - Sanzione di 500.000 al Titolare del trattamento
- L'Autorità ha comminato, inoltre, con separato provvedimento una [sanzione di 40mila euro alla società fornitrice del sistema](#) per i trattamenti effettuati in qualità di autonomo titolare, in particolare, con riguardo alla prenotazione di servizi sanitari da parte degli utenti e alla manutenzione del sistema per conto dei clienti, nei casi in cui tale attività comportasse il trattamento di dati personali di utenti e dipendenti.
- È stato inoltre adottato un [provvedimento di avvertimento](#) nei confronti della medesima società fornitrice e di tutti i soggetti pubblici e privati che utilizzano il sistema "TuPassi" in ordine alla possibilità che il suo utilizzo, con le modalità già censurate dal Garante, possa violare il Regolamento, ingiungendo alla società di avviare con loro i necessari aggiornamenti per rendere il sistema conforme alla disciplina in materia di protezione dati, secondo le indicazioni del Garante



Home - Istituzioni e diritto - AMMINISTRATIVO E PROCESSO



ISTITUZIONI E DIRITTO

PRIVACY

13/02/2023




RICERCA AVANZATA

## Il trattamento dei dati in ambito sanitario: il punto di vista del Garante

Il Garante per la protezione dei dati personali richiama l'attenzione delle Regioni e degli enti sulla delicatezza dei trattamenti di dati sanitari, sul ruolo centrale della formazione degli operatori e della vigilanza.

di Mauro Alovisio - Avvocato

ISTITUZIONI E DIRITTO

### NOTIZIE CORRELATE

- La realizzazione di un murales a carattere decorativo va qualificata come intervento di manutenzione straordinaria
- Le Sezioni Unite intervengono sul potere di proroga delle concessioni demaniali marittime
- L'iscrizione nell'Elenco degli Arbitri è incompatibile con la carica di Consigliere del COA?
- Violenza nelle scuole: in difesa di docenti e personale, il Ministero



Caro Lettore, per consultare questo documento è necessario essere abbonati. [ABBONATI SUBITO](#) e potrai accedere a tutti i contenuti del sito, se sei già registrato effettua il [LOGIN](#).



AGGIUNGI  
A RACCOLTA

Grazie per attenzione

Per informazioni e contatti

[mauro.alovisio@unito.it](mailto:mauro.alovisio@unito.it)