UNIVERSITÀ DEGLI STUDI DI PALERMO

AREA AFFARI GENERALI E LEGALI
Settore Affari Legali Generali. Privacy e trasparenza

Titolo I	Classe 6	Fascicolo
N. 15860	del 02-03-2015	
UOR Set 45	CC	RPA

Al Direttore Generale

Ai Presidenti delle Scuole

Ai Direttori di Dipartimento e Centri Interdipartimentali

Ai Responsabili dei Poli Didattici

Al Direttore di UNINETLAB

Ai Dirigenti

Al Responsabile Informatico d'Ateneo

Ai Responsabili di Settori e Servizi

LORO SEDI

Oggetto: Provvedimento generale prescrittivo dell'Autorità Garante per la protezione dei dati personali del 12 novembre 2014 in tema di biometria.

L'Autorità Garante per la protezione dei dati personali, nell'adunanza del 12 novembre 2014, ha emanato il **Provvedimento generale prescrittivo in tema di biometria** (n. 513, doc. web n. 3556992). Al Provvedimento generale sono allegate le **Linee guida** (doc. web n. 3563006) e un **modulo** (Allegato B, doc. web n. 3563019) per la comunicazione all'Autorità di violazioni dei sistemi biometrici. Il provvedimento è stato pubblicato sulla Gazzetta Ufficiale del 12 novembre 2014 n. 280 ed è rinvenibile sul sito web dell'Autorità.

L'intervento del Garante si è reso necessario alla luce della crescente diffusione, anche presso le amministrazioni pubbliche, di dispositivi atti al trattamento di **dati c.d. biometrici**, come le impronte digitali, la topografia della mano o le caratteristiche della firma autografa per il controllo degli accessi, per l'autenticazione degli utenti (anche su pc e tablet) o per la sottoscrizione di documenti informatici.

Con il Provvedimento generale in oggetto l'Autorità ha inteso pertanto fornire un **quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale** nell'utilizzo di particolari tipi di dati biometrici, al fine di mantenere alti livelli di sicurezza.

In particolare, anche in un'ottica semplificatrice, nel Provvedimento generale vengono individuate **alcune tipologie di trattamento** che, per le specifiche finalità perseguite, presentano un livello ridotto di rischio e per le quali, dunque, **non sarà più necessario attivare, come avveniva**

Salita Intendenza, 1 – ex Hotel de France, – 90133 Palermo - telef. 091/23893625 - 4 , ufficio privacy - telef. 091/23893869
email legale.generale@unipa.it - email privacy@unipa.it fax 091/23860883

in passato, la procedura di verifica preliminare da parte della stessa Autorità (rimangono comunque esclusi dalle modalità semplificate individuate nel provvedimento i trattamenti che prevedono la realizzazione di archivi biometrici centralizzati, per i quali continuerà ad essere obbligatorio effettuare tale adempimento).

All'interno del Provvedimento vengono individuate le seguenti tipologie di trattamento biometrico:

- **Autenticazione informatica (Punto 4.1)**: le caratteristiche biometriche dell'impronta digitale o dell'emissione vocale di una persona possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici, nel rispetto delle condizioni prescritte (vedi lettere da a) a j)).
- **Controllo di accesso fisico ad aree "sensibili" e utilizzo di apparati e macchinari pericolosi (Punto 4.2):** le caratteristiche dell'impronta digitale o della topografia della mano potranno essere trattate per consentire l'accesso ad aree e locali ritenuti "sensibili", oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati, osservando i prescritti accorgimenti (vedi lettere da a) a j)).
- **Scopi facilitativi (Punto 4.3):** l'impronta digitale e la topografia della mano potranno essere utilizzate anche per consentire l'accesso fisico di utenti ad aree fisiche (es. biblioteche). Presupposto di legittimità del trattamento, in questo caso, è dato dal consenso effettivamente libero degli interessati (in tutti gli altri casi le PP.AA. non devono acquisire il consenso). Dovranno comunque essere rispettate le condizioni di cui alle lettere da a) a g) del provvedimento e **previste modalità alternative** per l'erogazione del servizio per chi rifiuta di far utilizzare i propri dati biometrici.
- **Sottoscrizione di documenti informatici (Punto 4.4):** l'analisi dei dati biometrici associati all'apposizione a mano libera di una firma autografa potrà essere utilizzata per la firma elettronica avanzata. Dovranno comunque essere rispettate le condizioni di cui alle lettere da a) a k) ed essere **resi disponibili sistemi alternativi** (cartacei o digitali) **di sottoscrizione**, che non comportino l'utilizzo di dati biometrici.

Nell'effettuare i suddetti trattamenti, **dovranno comunque essere osservate rigorosamente le condizioni e le misure di sicurezza** individuate dal Garante, rispettando i presupposti di legittimità previsti dal D. Lgs. 196/03 – Codice in materia di trattamento dei dati personali e richiamati nel capitolo 4 delle Linee guida, in particolare per quanto riguarda l'**informativa** da rilasciare sempre agli interessati sui loro diritti, sugli scopi e le modalità del trattamento, ai sensi dell'Art. 13 del Codice.

Ogni sistema di rilevazione dovrà poi essere configurato in modo tale da raccogliere un numero limitato di informazioni (**principio di minimizzazione**), escludendo l'acquisizione di dati ulteriori rispetto a quelli necessari per il conseguimento della finalità perseguita (ad esempio, in caso di autenticazione informatica, i dati biometrici non dovranno essere trattati in modo da poter desumere anche informazioni di natura sensibile dell'interessato).

Tra le numerose misure di sicurezza individuate dal Garante vi è quella che obbliga a **cifrare il riferimento biometrico con tecniche crittografiche**, con una lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati. Particolare attenzione è inoltre rivolta alla messa in sicurezza dei dispositivi mobili (come tablet o pc) che potrebbero più facilmente essere compromessi o smarriti.

Si richiama, infine, l'attenzione delle SS.LL. su quanto previsto al punto 3 ("Comunicazione di violazione dei dati biometrici") del Provvedimento in argomento. Infatti, anche al fine di

prevenire eventuali furti di identità biometrica, **tutte le violazioni dei dati o gli incidenti informatici ("data breaches")** che possano avere un impatto significativo sui sistemi biometrici o sui dati personali custoditi (quali, a titolo esemplificativo e non esaustivo, accessi abusivi, azioni di malware, ecc.) **dovranno essere comunicati al Garante entro 24 ore dalla scoperta**, così da consentire di adottare opportuni interventi a tutela delle persone interessate. A tale scopo è stato predisposto dall'Autorità un modulo (Allegato B, doc. web n. 3563019) che consente di semplificare il predetto adempimento e che dovrà pervenire all'Autorità secondo le modalità previste al punto 3 del Provvedimento generale.

Allo stato, non risultano comunicati al Settore Affari legali generali. Privacy e trasparenza di questo Ateneo trattamenti di dati biometrici da parte delle Strutture universitarie; tuttavia, allo scopo di uniformare alle prescrizioni del Garante gli eventuali trattamenti del tipo sopradescritto che si rendesse necessario avviare presso le Strutture di propria competenza, si trasmette alle SS.LL., in allegato, il Provvedimento Generale in oggetto, unitamente alle Linee guida e al modulo per la comunicazione all'Autorità di violazioni dei sistemi biometrici.

IL RETTORE
(Prof. Roberto Lagalla)