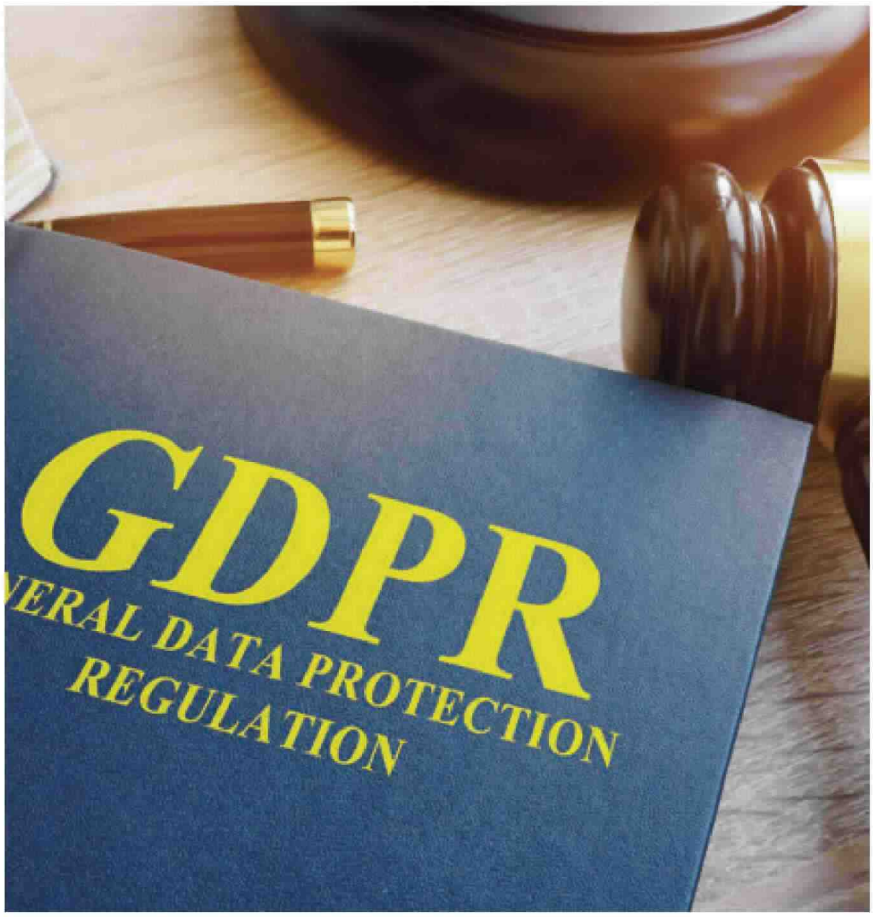
ISPEZIONI ALLA PORTA: ECCO COSA FARE

I controlli della Guardia di finanza o del Garante per il trattamento dei dati personali saranno costanti e non sempre comunicati per tempo. Ecco un vademecum per evitare errori che potrebbero costare caro alle aziende



"Se il padrone di casa sapesse a quale ora viene il ladro, non si lascerebbe scassinare la casa. Anche voi tenetevi pronti..." recita una nota parabola del Vangelo che può tornare utile anche per le più laiche ispezioni delle autorità in materia di tutela privacy. Perché ora che le regole del gioco stanno cambiando, anche i controlli potrebbero aumentare. E non si sa quando verranno a bussare alla porta per chiedere conto delle attività di un'azienda.

PRIMO PUNTO: ESSERE PRONTI

Se si dovesse immaginare un vademecum di comportamento, in questo caso, la prima regola sarebbe: essere pronti a gestire un'ispezione del Garante per la protezione dei dati personali. General-

mente le ispezioni sono precedute da segnalazioni o ricorsi. Oppure sono iniziative del Garante all'interno di una road map ben definita.
Tuttavia se un'azienda viene contattata dall'autorità preposta per avere informazioni specifiche sulla propria attività, allora è probabile che di lì a poco ci sarà una visita ispettiva. Magari di persona. Nei casi meno gravi, delle visite di routine è la Gdf a occuparsene. In quelli più gravi sono gli ispettori del Garante, senza il supporto del nucleo della Guardia di finanza. Secondo quanto scritto su questo giornale dall'avvocato Gianluigi Marino, partner di Osborne-Clarke (AboutPharma n°154, pagine 90-91), se l'ispezione è condotta in prima persona dagli ispettori, è possibile aspettarsi che la situazione diventi controversa. L'ispezione potrebbe portare alla luce altre possibili violazioni. Quindi, in base al soggetto che provvede agli accertamenti, si comprende il maggiore o minore livello di consapevolezza dell'autorità riguardo i problemi dell'azienda ispezionata.

SECONDO PUNTO: TROVARE LE RISPOSTE GIUSTE

I controlli possono essere comunicati (il giorno prima) o avvenire a sorpresa. Prima dell'ispezione viene richiesto un documento chiamato "richiesta di informazioni". Con questo elemento, notificato al momento dell'accesso in sede, si chiede conto di tutti gli adempimenti legislativi e regolamentari in materia di dati personali. Come viene raccolto il consenso? Come viene data l'informativa agli interessati? Come vengono contrattualizzati i responsabili esterni del trattamento? Tutte domande a cui va trovata una risposta.

TERZO PUNTO: AVERE UNA FIGURA CHE SEGUA LE ISPEZIONI

Le procedure interne devono essere snelle, veloci. Gli onori di casa vanno fatti subito. Generalmente, ad adempiere a questo compito sono il responsabile interno della privacy, il capo ufficio legale, il capo della funzione compliance o il Dpo.

Adesso si è tutti più "responsabili"

Il termine "accountability", cioè responsabilizzazione, è il concetto intorno al quale ruota il nuovo regolamento europeo sulla privacy. "Da un mondo di compliance si passa al concetto di accountability – ha detto il colonnello Marco Menegazzo, comandante del Nucleo speciale Privacy della Guardia di finanza durante il convegno "La privacy nella sanità: il sistema sanzionatorio e l'attività ispettiva", organizzato da Scudomed e AreaMedici il 17 aprile a Roma – e il titolare del trattamento deve essere in grado di comprovare ciò che è stato fatto. In sede ispettiva, noi lo traduciamo letteralmente in 'rendere conto'", ha spiegato il colonnello. "La Gdf deve fotografare lo stato dell'arte e poi, a differenza del passato, rimettere all'autorità le valutazioni di competenza per eventuali sanzioni. Al titolare del trattamento sono affidati una serie di compiti che se non vengono svolti diventano oggetto di sanzione. Basta, ad esempio, non nominare il data protection officer (Dpo) per essere passibili di sanzioni". Il margine di errore è quindi minimo.

QUARTO PUNTO: VERBALIZZARE QUANTO AVVIENE E QUANTO VIENE DETTO

Va tutto trascritto, registrato e controllato. Meglio riservarsi di verificare la correttezza di quanto dichiarato. Meglio ancora se a vagliare il tutto è un legale interno alla società o un consulente esterno.

QUINTO PUNTO: AVERE UNA COMPLIANCE PRIVACY BEN RODATA

Sarà più facile accedere alla documentazione richiesta. Tuttavia sono previsti quattordici giorni per l'invio del materiale. Niente di preoccupante se nell'immediato non vengono soddisfatte le richieste degli ispettori. Accade di frequente.

PUNTO SESTO: CONSIDERARE LA DURATA DELLE OPERAZIONI

Le indagini durano circa due o tre giorni, quindi è necessario che la figura aziendale preposta a seguirle stenda un rapporto esaustivo su quanto è accaduto.

PUNTO SETTE: MAI RILASCIARE DOCUMENTI ORIGINALI

Meglio solo le copie. Inoltre bisogna prendere nota delle banche dati ispezionate, farsi rilasciare una copia del verbale dall'ispettore, dare sempre informazioni veritiere e, in caso di dubbi, meglio non rispondere e rimandare ad accertamenti successivi. Come agli esami universitari, meglio tacere che dare una risposta scorretta. In caso di documentazione riservata è bene cancellare o rendere anonimi dati sensibili che non si vogliono rendere conoscibili all'ispettore. Per esempio, i termini economici degli accordi. Marino si chiede: "le organizzazioni saranno sufficientemente responsabilizzate da reggere all'impatto del Gdpr e delle nuove ondate di ispezioni dei prossimi semestri?".

PUNTO OTTO: NON CI SARANNO DEROGHE

Nelle settimane scorse è circolata una notizia, poi rivelatasi falsa, su un possibile periodo transitorio da concedere alle aziende non compliant dopo la data del 25 maggio 2018. Il Garante è dovuto intervenire pubblicamente per smentire qualsiasi informazione relativa a questo "periodo ponte" e confermare l'effettiva entrata in vigore il 25 maggio. Anzi, a dirla tutta, una sorta di periodo transitorio c'è già stato. Il Gdpr è entrato in vigore nel 2016, ma le istituzioni europee hanno deciso di concedere ulteriori due anni per consentire l'adeguamento alle aziende.

Parole chiave
Gdpr, privacy, big data, sicurezza
Aziende/Istituzioni
Idc, Scudomed, OsborneClarke, Deloitte, Lloyd's, Sas, Politecnico di Milano, studio legale Stefanelli&Stefanelli, Garante della privacy, Guardia di finanza