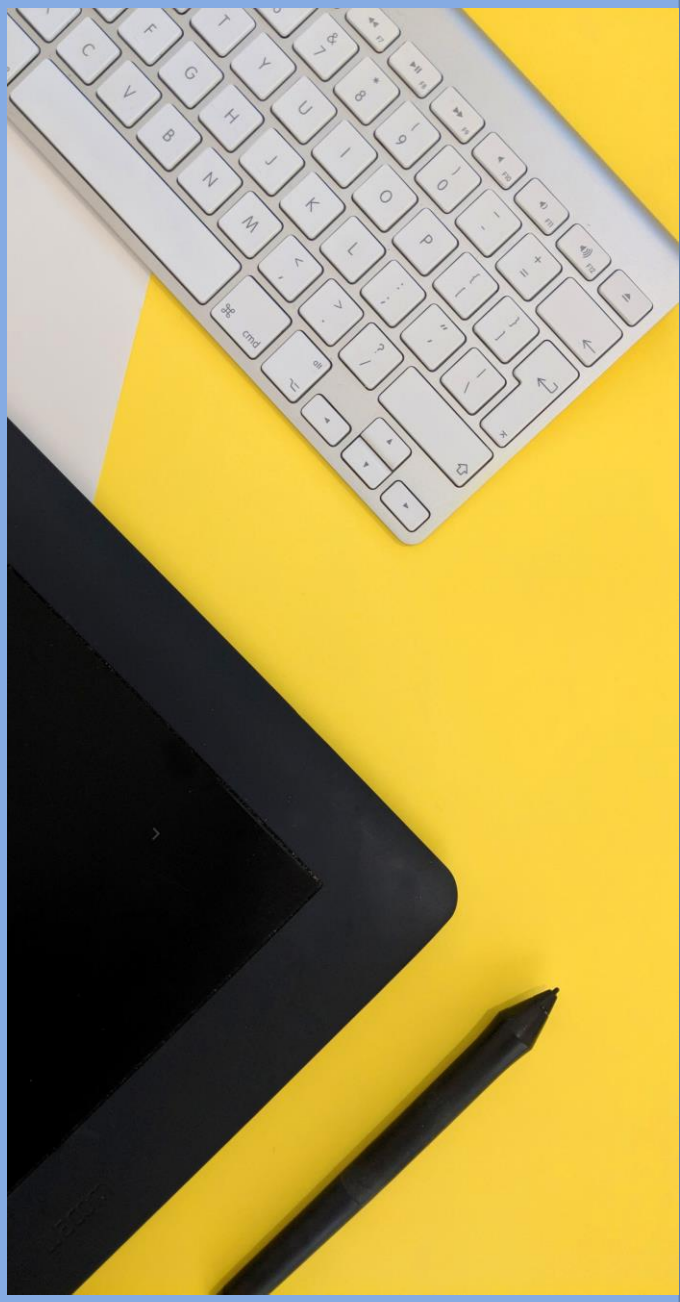
Bird & Bird

GDPR e certificazioni

Approvato il primo schema di certificazione per le attività di trattamento dei dati personali

14 ottobre 2022



GDPR e certificazioni: approvato il primo schema di certificazione per le attività di trattamento dei dati personali

Lo scorso 10 ottobre, l'European Data Protection Board ("**EDPB**") ha fornito parere favorevole ai criteri di certificazione proposti da Europrivacy e sottoscritti dall'Autorità di controllo del Lussemburgo, approvando il primo schema di certificazione paneuropeo e riconoscendone l'applicabilità a tutti i titolari e responsabili del trattamento all'interno del territorio dell'Unione Europea.

1. Il quadro normativo di riferimento

L'art. 42 del Regolamento Europeo 2016/679 sulla protezione dei dati personali ("**GDPR**" o "**Regolamento**")[1] disciplina le c.d. certificazioni, il cui scopo, come chiarito dal paragrafo 1 dello stesso articolo, è quello di agevolare titolari e responsabili del trattamento nel dimostrare il corretto adempimento agli obblighi cui sono soggetti e, più in generale, la propria conformità al Regolamento stesso.

Nello specifico, la norma prevede che le Autorità di controllo dei singoli Stati membri o, in alternativa, i c.d. organismi di certificazione[2] di cui al successivo art. 43 GDPR, possano rilasciare ai titolari o ai responsabili che ne facciano richiesta una certificazione che attesti la conformità di una o più attività di trattamento alla disciplina dettata dal GDPR, previo espletamento di una specifica procedura.

Nelle linee-guida 1/2018, l'EDPB aveva peraltro chiarito che l'oggetto della certificazione può variare notevolmente, ricomprendendo tanto una singola operazione di trattamento, quanto più operazioni. Inoltre, nel caso in cui uno o più trattamenti configurino un servizio o un prodotto, questi possono rappresentare l'oggetto stesso della certificazione. In ogni caso, la certificazione rilasciata deve indicare chiaramente il perimetro della stessa.

Il conseguimento della certificazione (che può essere rilasciata per un periodo massimo di tre anni, salva la possibilità di rinnovo) non riduce, tuttavia, la responsabilità del titolare o del responsabile riguardo alla conformità al GDPR (art. 42, paragrafo 2).

L'adesione a un meccanismo di certificazione rappresenta inoltre uno degli elementi che concorrono a definire il *quantum* in caso di sanzioni pecuniarie inflitte dalle Autorità di controllo nazionali, al pari, *ex multis*, della natura, della gravità, della durata della violazione e del grado di cooperazione con l'autorità di controllo.

2. Il parere dell'EDPB e il contenuto dello schema di certificazione

Ai sensi dell'art. 64, paragrafo 1, lett. c) GDPR, l'approvazione di uno schema di certificazione deve essere preceduta dal parere favorevole dell'EDPB. Nel rispetto, dunque, del meccanismo di coerenza, lo scorso 10 ottobre l'EDPB ha pubblicato l'*Opinion* 28/2022, dichiarando lo schema di certificazione proposto da

[1] "*La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati*" (art. 42, paragrafo 5, GDPR).

[2] Si tratta di soggetti terzi indipendenti accreditati, ai sensi dell'art. 43, paragrafo 3 GDPR, in base ai requisiti approvati dall'Autorità di controllo competente o dall'EDPB.

Europrivacy idoneo ad attestare la conformità dei trattamenti di dati personali rientranti nell'ambito di applicazione dello stesso Regolamento.

Si tratta di uno schema di carattere generale, volto a includere diverse attività di trattamento poste in essere da titolari o responsabili del trattamento che operano in vari settori di mercato all'interno del territorio dell'Unione Europea, pur essendone espressamente esclusi i trattamenti aventi ad oggetto dati genetici.

L'EDPB ritiene che i criteri previsti dallo schema di certificazione approvato siano idonei a coprire l'intero spettro degli obblighi a cui titolari e responsabili sono generalmente soggetti ai sensi del GDPR, sebbene la loro applicabilità in concreto potrà variare a seconda del ruolo e delle responsabilità proprie di ciascun richiedente.

In particolare, l'EDPB distingue fra "*Core criteria*" e "*TOMs checks and control*", definendo questi ultimi come quelli volti a indagare l'adeguatezza delle misure tecniche e organizzative poste in essere per garantire la sicurezza dei dati personali (*e.g.*, l'individuazione chiara dei ruoli e delle responsabilità in materia di *privacy*, l'adozione di procedure adeguate per la gestione di eventuali violazioni di dati personali, l'effettuazione di valutazioni d'impatto sulla protezione dei dati, *etc*.). All'interno di questa seconda categoria viene inoltre identificata una serie di misure specifiche, la cui implementazione è valutata esclusivamente nel caso di trattamenti aventi ad oggetto categorie speciali di dati personali, dati relativi a condanne penali e reati o dati di minori.

Nell'ambito dei "*Core criteria*" rientrano, invece, le verifiche concernenti le categorie di dati oggetto di trattamento, l'adempimento agli obblighi informativi e di tenuta del registro delle attività di trattamento, la liceità del trattamento, il rispetto dei principi di cui all'art. 5 GDPR e dei principi di *privacy-by-design* e *by-default*, nonché l'osservanza delle norme relative al trasferimento dei dati verso Paesi terzi od organizzazioni internazionali e ai diritti degli interessati. Anche la conformità alla disciplina in materia di *cookie* e profilazione è espressamente annoverata fra i criteri rilevanti.

Lo schema prevede inoltre che, ai fini dell'ottenimento della certificazione, il titolare o responsabile del trattamento richiedente dovrà designare un Responsabile della Protezione dei Dati Personali ai sensi dell'art. 37 GDPR, anche qualora non vi fosse tenuto a norma dell'articolo richiamato.

Infine, qualora la legislazione interna a ciascun Stato membro dovesse prevedere degli obblighi specifici in capo a titolari e/o responsabili operanti in particolari settori o con riguardo ad alcune attività di trattamento, l'organismo di certificazione valuterà altresì l'adeguatezza delle misure adottate per garantire il rispetto di tali obblighi.

3. Conclusioni

Lo schema di certificazione approvato dall'EPDB rappresenta uno strumento di particolare importanza a favore di aziende ed enti operanti all'interno del territorio dell'Unione Europea, dal momento che, grazie alla loro adesione allo schema di certificazione stesso, questi saranno in grado di dimostrare più agevolmente il rispetto degli obblighi, le garanzie sufficienti e la conformità ai requisiti di protezione dei dati.

In tale ottica, l'adesione a uno schema di certificazione può rappresentare altresì uno strumento utile a rafforzare la reputazione di prodotti e servizi *data driven* sul mercato e nei rapporti con gli interessati, oltre che un parametro di valutazione ai fini della quantificazione delle eventuali sanzioni pecuniarie in caso di procedimenti sanzionatori delle Autorità di controllo nazionali.

Resta, tuttavia, inteso che l'adesione a uno schema di certificazione non esime titolari e responsabili da una costante valutazione dei propri processi e delle connesse attività di trattamento di dati personali, e men che meno è in grado di ridurre un'eventuale responsabilità giuridicamente rilevante in ipotesi di trattamento illecito dei dati personali.

Contatti

Adriano D'Ottavio

Counsel

+39 0669667000
adriano.dottavio@twobirds.com

Debora Stella

Counsel

+39 0230356000
debora.stella@twobirds.com

Matteo Susta

Associate

+39 0669667000
matteo.susta@twobirds.com

Elena Mandarà

Trainee Associate

+39 0669667000
elena.mandara@twobirds.com

twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai • Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Luxembourg • Lyon • Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Singapore • Stockholm • Sydney • Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority (SRA) with SRA ID497264. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.