Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876]

- English version

VEDI ANCHE

- Allegato 1 - Scheda di sintesi

- Comunicato stampa del 10 luglio 2021

- Pagina tematica COOKIE

[doc. web n. 9677876]

Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021
(Pubblicato sulla Gazzetta Ufficiale n. 163 del 9 luglio 2021)

Registro dei provvedimenti
n. 231 del 10 giugno 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

VISTA la direttiva 2002/21/CE del 7 marzo 2002, del Parlamento europeo e del Consiglio, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (c.d. direttiva quadro), come successivamente modificata e integrata;

VISTA la direttiva 2002/58/CE del 12 luglio 2002, del Parlamento europeo e del Consiglio, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. direttiva ePrivacy), come modificata dalla direttiva 2009/136/CE del 25 novembre 2009, del Parlamento europeo e del Consiglio;

VISTO il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

VISTO il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196), come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al citato Regolamento;

VISTO il decreto legislativo 28 maggio 2012, n. 69 recante "Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori";

VISTI il Parere del Gruppo di lavoro "Art. 29" (di seguito WP29) n. 04/2012 in materia di Cookie Consent Exemption, adottato il 7 giugno 2012, ed il Working Document del medesimo WP29 n. 02/2013 providing guidance on obtaining consent for cookies, adottato il 2 ottobre 2013, nonché le Linee Guida del WP29 sul consenso ai sensi del Regolamento (UE) 2016/679 adottate il 10 aprile 2018, ratificate dal Comitato europeo per la Protezione dei dati personali (di seguito, EDPB) il 25 maggio 2018 e sostituite, da ultimo, dalle Guidelines 05/2020 on consent under Regulation 2016/679 adottate il 4 maggio 2020;

VISTO il Parere dell'EDPB n. 05/2019 del 12 marzo 2019 sulle interrelazioni tra la direttiva e-Privacy ed il Regolamento, con particolare riguardo alle competenze, ai compiti ed ai poteri delle Autorità di protezione dati;

VISTO il provvedimento del Garante n. 229, dell'8 maggio 2014, relativo alla "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie", pubblicato nella Gazzetta Ufficiale della Repubblica italiana del 3 Giugno 2014, serie Generale, n. 126, del 3 giugno 2014;

VISTE le FAQ in materia di informativa e consenso per l'uso dei cookie del 3 dicembre 2014 ed i "Chiarimenti in merito all'attuazione della normativa in materia di cookie" del 5 giugno 2015, pubblicati dall'Autorità nel proprio sito web www.garanteprivacy.it;

VISTO il provvedimento del Garante n. 161, del 19 marzo 2015, recante le "Linee guida in materia di trattamento di dati personali per profilazione on line", pubblicato nella Gazzetta Ufficiale della Repubblica italiana, serie Generale, n. 103 del 6 maggio 2015;

VISTA la deliberazione del Garante n. 255 del 26 novembre 2020 (doc. web n. 9498472) con la quale è stato adottato uno schema di "Linee guida sull'utilizzo di cookie e altri strumenti di tracciamento" (allegato 1, doc. web 9501061) nonché l'unita scheda di sintesi (allegato 2, doc. web 9501097), con contestuale avvio, mediante pubblicazione del relativo avviso nella Gazzetta Ufficiale della Repubblica Italiana – serie generale, n. 307 dell'11 dicembre 2020, di una consultazione pubblica sulle misure ivi indicate;

VISTI gli esiti di tale consultazione pubblica, tesa ad "acquisire osservazioni e proposte riguardo alle predette Linee guida";

CONSIDERATI, in particolare, i contributi pervenuti, nel previsto termine di 30 giorni, da diverse associazioni di categoria, dagli operatori e da soggetti appartenenti al mondo imprenditoriale, da associazioni di consumatori, rappresentanti dell'Accademia e singoli interessati;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 del 28 giugno 2000;

RELATORE l'avv. Guido Scorza;

PREMESSO

1. Considerazioni preliminari

Le presenti Linee guida hanno innanzitutto una funzione ricognitiva in relazione al diritto applicabile alle operazioni di lettura e di scrittura all'interno del terminale di un utente, con specifico riferimento all'utilizzo di cookie e di altri strumenti di tracciamento, nonché l'obiettivo di specificare, al riguardo, le corrette modalità per la fornitura dell'informativa e per l'acquisizione del consenso on-line degli interessati, ove necessario, alla luce della piena applicazione del Regolamento (UE) 2016/679 (di seguito, Regolamento).

Il quadro giuridico di riferimento è infatti, ad oggi, costituito tanto dalle disposizioni della direttiva 2002/58/CE (c.d. direttiva ePrivacy) e successive modifiche, come recepita nell'ordinamento nazionale all'art. 122 del d.lgs. 30 giugno 2003, n. 196 (di seguito Codice), quanto dal Regolamento, per ciò che concerne specificamente la nozione di consenso di cui agli artt. 4, punto 11) e 7 e al considerando 32, come da ultimo interpretati dalle Linee Guida del WP29 adottate il 10 aprile 2018, ratificate dal Comitato europeo per la Protezione dei dati personali (di seguito, EDPB) il 25 maggio 2018 e sostituite, da ultimo, dalle Guidelines 05/2020 on consent under Regulation 2016/679 adottate il 4 maggio 2020.

In proposito il Garante, come è noto, ha già adottato un provvedimento (n. 229, dell'8 maggio 2014), volto ad "individuare le modalità semplificate per rendere l'informativa online agli utenti sull'archiviazione dei c.d. cookie sui loro terminali da parte dei siti Internet visitati", come pure a "fornire idonee indicazioni sulle modalità con le quali procedere all'acquisizione del consenso degli stessi, laddove richiesto dalla legge", le cui indicazioni necessitano ora di essere integrate e precisate, in particolare con riferimento a taluni, specifici aspetti (al fine di agevolare i titolari del trattamento nella corretta applicazione del citato quadro regolamentare come specificato dal richiamato provvedimento del maggio 2014 e dalle presenti Linee guida, si allega a queste ultime una tabella riassuntiva delle indicazioni contenute in entrambi i provvedimenti).

Da un lato deve essere infatti considerato che il Regolamento, come precisato all'art. 95, "non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE", la quale espressamente prevede, all'art. 1, par. 2, che "le disposizioni della presente direttiva precisano e integrano [il Regolamento (EU) 2016/679] …".

D'altro canto, non può essere sottovalutato come il Regolamento abbia inteso ampliare e rafforzare il potere dispositivo e di controllo della persona riguardo al trattamento delle sue informazioni personali, in particolar modo integrando la definizione di consenso contenuta nella precedente direttiva 95/46/CE, chiarendo che la manifestazione di volontà dell'interessato al trattamento dei suoi dati personali deve essere, oltre che – come appunto già nel vigore della direttiva – libera, specifica ed informata, anche "inequivocabile"[(1)], ma pure esigendo che l'obiettivo della concreta ed efficace attuazione dei principi di protezione dati venga conseguito sin dalla progettazione e attraverso impostazioni predefinite (cd. privacy by design e by default).

L'esigenza di un nuovo intervento del Garante è dovuta al lungo intervallo di tempo trascorso, alle novità normative frattanto intervenute e al monitoraggio che, anche per il tramite dei numerosi

reclami, segnalazioni e richieste di pareri, l'Autorità ha effettuato sulla concreta e talvolta non corretta implementazione delle regole menzionate – in particolare considerando gli effetti riscontrabili sull'esperienza di navigazione, sui diritti e sulle tutele degli interessati, come pure sulla operatività delle imprese e dei fornitori di servizi di comunicazione elettronica - nonché alla sempre crescente diffusione di nuove tecnologie caratterizzate da crescenti livelli di potenziali pervasività.

Infine, deve essere tenuta in considerazione l'evoluzione comportamentale degli stessi utenti della rete, sempre più orientati alla moltiplicazione delle proprie identità digitali come risultanti dall'accesso a plurimi servizi e funzioni disponibili e, in primo luogo, ai social network. Tale fenomeno comporta infatti il rischio che le informazioni personali oggetto di trattamento siano raccolte proprio incrociando i dati anche relativi all'utilizzo di funzionalità e servizi diversi, ai quali è possibile accedere utilizzando molteplici terminali (cd. enrichment), con l'effetto della creazione di profili sempre più specifici e dettagliati. Si impone, di conseguenza, la necessità di un quadro rafforzato di tutele maggiormente orientate a favorire e a rendere effettivo il controllo sulle informazioni personali oggetto di trattamento e, in definitiva, la capacità di autodeterminazione del singolo.

2. La funzione dei cookie

Il considerando 30 del Regolamento espressamente afferma che "Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

Come è noto, i cookie sono di regola stringhe di testo che i siti web (cd. Publisher, o "prime parti") visitati dall'utente ovvero siti o web server diversi (cd. "terze parti") posizionano ed archiviano – direttamente, nel caso dei publisher e indirettamente, cioè per il tramite di questi ultimi, nel caso delle "terze parti" - all'interno di un dispositivo terminale nella disponibilità dell'utente medesimo.

I terminali cui ci si riferisce sono, ad esempio, un computer, un tablet, uno smartphone, ovvero ogni altro dispositivo in grado di archiviare informazioni. Già oggi, e ancor più in futuro, tra essi occorre annoverare anche i cd. dispositivi IoT (Internet of Things, o Internet delle cose), i quali sono progettati per connettersi alla rete e tra loro per fornire servizi di varia natura, non necessariamente limitati alla mera comunicazione.

I software per la navigazione in internet e il funzionamento di questi dispositivi, ad esempio i browser, possono memorizzare i cookie e poi trasmetterli nuovamente ai siti che li hanno generati in occasione di una successiva visita del medesimo utente, mantenendo così memoria della sua precedente interazione con uno o più siti web.

Le informazioni codificate nei cookie possono includere dati personali, come un indirizzo IP, un nome utente, un identificativo univoco o un indirizzo e-mail, ma possono anche contenere dati non personali, come le impostazioni della lingua o informazioni sul tipo di dispositivo che una persona sta utilizzando per navigare nel sito.

I cookie possono dunque svolgere importanti e diverse funzioni, tra cui il monitoraggio di sessioni, la memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al server, l'agevolazione nella fruizione dei contenuti online etc. Possono ad esempio essere impiegati per tenere traccia degli articoli in un carrello degli acquisti online o delle informazioni utilizzate per la compilazione di un modulo informatico.

Se da un lato è tramite i cookie che è possibile consentire, tra l'altro, alle pagine web di caricarsi

più velocemente, come pure instradare le informazioni su una rete - in linea dunque con adempimenti strettamente connessi alla operatività stessa dei siti web -, sempre attraverso i cookie è possibile anche veicolare la pubblicità comportamentale (c.d. “behavioural advertising”) e misurare poi l’efficacia del messaggio pubblicitario, ovvero conformare tipologia e modalità dei servizi resi ai comportamenti dell’utente oggetto di precedente osservazione.

3. Altri strumenti di tracciamento

Il medesimo risultato può essere conseguito anche mediante l’utilizzo di altri strumenti (la totalità dei quali può essere distinta tra i c.d. “identificatori attivi”, come appunto i cookie, e “passivi”, questi ultimi presupponendo la mera osservazione), che consentono di effettuare trattamenti analoghi a quelli sopra indicati.

Tra gli strumenti “passivi” è ricompreso il fingerprinting, ossia quella tecnica che permette di identificare il dispositivo utilizzato dall’utente tramite la raccolta di tutte o alcune delle informazioni relative alla specifica configurazione del dispositivo stesso adottata dall’interessato. Tale tecnica può essere utilizzata per il conseguimento delle medesime finalità di profilazione tesa anche alla visualizzazione di pubblicità comportamentale personalizzata ed all’analisi e monitoraggio dei comportamenti dei visitatori di siti web, ovvero per conformare tipologia e modalità dei servizi resi ai comportamenti dell’utente oggetto di precedente osservazione. Per tali ragioni, il fingerprinting e gli ulteriori strumenti di tracciamento devono dunque essere ricompresi nell’ambito di applicazione delle presenti Linee guida.

Sussiste tuttavia una non trascurabile differenza, sulla quale l’Autorità intende porre l’accento, tra l’impiego di una tecnica attiva quale quella relativa ai cookie ed una passiva, come quella relativa al fingerprinting.

Nel primo caso, infatti, l’utente che non intenda essere profilato, oltre ovviamente a poter rifiutare il proprio consenso, o a ricorrere alle tutele di carattere giuridico connesse all’esercizio dei diritti di cui al Regolamento, ha anche la possibilità pratica di rimuovere direttamente i cookie, in quanto archiviati all’interno del proprio dispositivo.

Diversamente, con riguardo al fingerprinting e agli altri identificatori “passivi”, l’utente non dispone di strumenti autonomamente azionabili, dovendo necessariamente far ricorso all’azione del titolare. Ciò in quanto quest’ultimo fa uso di una tecnica di lettura che non presuppone l’archiviazione di informazioni all’interno del dispositivo dell’utente, bensì la mera osservazione delle configurazioni che lo contraddistinguono rendendolo identificabile, ed il cui esito si sostanzia in un “profilo” che resta nella sola disponibilità del titolare, cui l’interessato non ha, ovviamente, alcun accesso libero e diretto e del quale potrebbe, prima ancora, non avere neppure consapevolezza.

4. La classificazione di cookie ed altri strumenti di tracciamento

I cookie e, in buona misura, gli altri strumenti di tracciamento possono avere caratteristiche diverse sotto il profilo temporale e dunque essere considerati in base alla loro durata (di sessione o permanenti), ovvero dal punto di vista soggettivo (a seconda che il publisher agisca autonomamente o per conto della “terza parte”).

E tuttavia la classificazione che risponde alla ratio della disciplina di legge e dunque anche alle esigenze di tutela della persona, è quella che si basa, in definitiva, su due macro categorie:

- i cookie tecnici, utilizzati al solo fine di “effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio” (cfr. art. 122, comma 1 del Codice);

- i cookie di profilazione, utilizzati per ricondurre a soggetti determinati, identificati o identificabili, specifiche azioni o schemi comportamentali ricorrenti nell'uso delle funzionalità offerte (pattern) al fine del raggruppamento dei diversi profili all'interno di cluster omogenei di diversa ampiezza, in modo che sia possibile al titolare, tra l'altro, anche modulare la fornitura del servizio in modo sempre più personalizzato al di là di quanto strettamente necessario all'erogazione del servizio, nonché inviare messaggi pubblicitari mirati, cioè in linea con le preferenze manifestate dall'utente nell'ambito della navigazione in rete.

Analogamente, anche gli altri identificatori possono essere catalogati secondo criteri diversi, dei quali il principale resta, tuttavia, la finalità per la quale vengono utilizzati: di natura "tecnica" o di natura "non tecnica", dovendosi intendere quest'ultima categoria in senso ampio, dal momento che l'attuale disciplina di legge, di cui in appresso, tesa alla tutela della confidenzialità delle comunicazioni elettroniche oltre che delle informazioni di carattere personale, è inequivocamente formulata secondo lo schema di una generale proibizione di trattamento dei dati degli interessati, salvo eccezioni rigorosamente e restrittivamente codificate, insuscettibili di estensione analogica.

5. Normativa applicabile

Per l'utilizzo di cookie e degli altri identificatori tecnici, in virtù della funzione assolta e nei limiti ed alle condizioni richiamate, il titolare del trattamento sarà assoggettato al solo obbligo di fornire specifica informativa, anche eventualmente inserita all'interno di quella di carattere generale, rientrando il loro impiego in una ipotesi codificata di esenzione dall'obbligo di acquisizione del consenso dell'interessato; i cookie e gli altri strumenti di tracciamento per finalità diverse da quelle tecniche potranno, invece, essere utilizzati esclusivamente previa acquisizione del consenso, comunque informato, del contraente o utente. E ciò in base alla norma tuttora applicabile alla fattispecie, ossia l'art. 122 del Codice, ai sensi del quale:

"1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate. Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.

2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.

2-bis. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente".

Questa disposizione è stata introdotta nell'ordinamento nazionale a seguito del recepimento della direttiva ePrivacy, precedente rispetto alla data della piena operatività degli effetti del Regolamento. Tale direttiva, al pari delle norme di diritto interno che la recepiscono, è tuttora applicabile allo specifico settore che riguarda i trattamenti di dati effettuati nell'ambito delle comunicazioni elettroniche (v., in proposito, il considerando 173 del Regolamento secondo cui "È

opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio …", nonché l'art. 2, lettera l), della direttiva quadro 2002/21/CE che ricomprende anche la direttiva ePrivacy nel novero delle "direttive particolari").

La successiva entrata in vigore del Regolamento impone tuttavia una indagine, innanzitutto tesa a ricercare il coordinamento tra le regole poste. Ad esclusione delle fattispecie disciplinate in via esclusiva ed esaustiva dalla direttiva ePrivacy, molte attività di trattamento devono infatti essere ricondotte all'ambito di applicazione tanto della direttiva quanto del Regolamento(2), con l'avvertenza tuttavia che, per la parte di potenziale sovrapposizione - in virtù del rapporto di genus a species sussistente tra le due discipline e di quanto disposto dall'art. 1, par. 2, della direttiva ePrivacy, il quale chiarisce proprio come le norme di questa precisino e integrino quelle del Regolamento - ogniqualvolta la direttiva renda più specifiche le prescrizioni del Regolamento, essa, in quanto lex specialis, dovrà essere applicata e prevarrà sulle (più generali) disposizioni del Regolamento. Queste ultime restano invece applicabili per tutte quelle fattispecie non specificamente previste dalla direttiva nonché per offrire, alle norme di questa, la cornice regolatoria di carattere generale entro cui collocarne i precetti(3).

Ad esempio, è nella direttiva ePrivacy che, nei casi previsti, si rinviene l'obbligo di acquisizione del consenso all'impiego di cookie e altri strumenti di tracciamento; ma è nel Regolamento che andranno ricercate le specifiche caratteristiche di quel consenso ai fini della sua validità e conformità alla disciplina generale.

Dalla ricostruzione normativa effettuata si trae una prima, importante conclusione: la disciplina di carattere speciale applicabile alla specie non contempla ulteriori basi giuridiche che rendano legittimo il trattamento se non in presenza del consenso dell'interessato ovvero al ricorrere di una delle ipotesi di deroga rispetto all'obbligo della sua raccolta previste proprio da tale disciplina speciale. In nessun caso sarà pertanto possibile invocare ad esempio, come è stato invece osservato nel corso delle verifiche effettuate su diversi siti web, la scriminante del legittimo interesse del titolare per giustificare il ricorso a cookie o altri strumenti di tracciamento.

6. Le modalità per l'acquisizione del consenso online alla luce di alcuni opportuni chiarimenti e nuove raccomandazioni

6.1 Il c.d. "scrolling" e il cookie wall

Il Garante ritiene che l'impianto teso alla individuazione della modalità tecnica per l'acquisizione del consenso online per il tracciamento a mezzo cookie (ovvero anche realizzato per il tramite di altri strumenti) illustrato nel menzionato provvedimento del maggio 2014 sia da ritenersi tuttora valido, pur nel mutato assetto normativo che privilegia ed impone ai titolari di agire in ossequio al nuovo regime di accountability (art. 5, par. 2, del Regolamento) consentendo loro, se del caso, anche l'adozione di modalità diverse attraverso cui assicurare la conformità alle regole e la tutela degli interessati.

Si reputa, tuttavia, opportuno fornire taluni chiarimenti in relazione all'utilizzo del c.d. scrolling ai fini della raccolta del consenso all'installazione e all'utilizzo di cookie ed altri strumenti di tracciamento nonché all'utilizzo del c.d. cookie wall.

Al riguardo, deve essere innanzitutto ricordato che, secondo il considerando 32 del Regolamento, "Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella

in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso".

L'EDPB ha, inoltre, chiarito (parere n. 5/2020, del 4 maggio 2020) che il semplice scrolling non è mai idoneo, di per sé, ad esprimere compiutamente la manifestazione di volontà dell'interessato volta ad accettare di ricevere il posizionamento, all'interno del proprio terminale, di cookie diversi da quelli tecnici e, dunque, non equivale, in sé considerato, al consenso "in nessuna circostanza" (4).

Il Garante condivide naturalmente l'opinione dell'EDPB: il semplice "scroll down" del cursore di pagina è inadatto in sé alla raccolta, da parte del titolare del trattamento, di un idoneo consenso all'installazione e all'utilizzo di cookie di profilazione ovvero di altri strumenti di tracciamento.

Non pare potersi escludere, tuttavia, che lo scrolling possa intervenire nella procedura di acquisizione del consenso e costituire non la sola, bensì una delle componenti di un più articolato processo che consenta comunque all'utente di segnalare al titolare del sito, con la generazione di un preciso pattern, una scelta inequivoca e consapevole, che sia al tempo stesso registrabile e dunque documentabile, volta a prestare il proprio consenso all'uso dei cookie o di altri strumenti di tracciamento, come richiesto dalle norme vigenti.

Tale conclusione risulta d'altro canto coerente, oggi, con il richiamato approccio regolamentare teso alla valorizzazione dell'accountability; pertanto, ed analogamente a quanto affermato con riferimento al potere di autonomia del titolare nell'identificazione delle soluzioni più appropriate per conseguire la conformità alle regole dei trattamenti di dati personali effettuati, il Garante invita i titolari a valutare con estremo rigore ogni possibile soluzione, anche di carattere tecnico, idonea ad essere interpretata e registrata come una forma di consenso espresso dall'utente per l'installazione dei cookie o per l'impiego di altri strumenti di tracciamento.

Affinché lo stesso risulti acquisito legittimamente, il medesimo titolare dovrà inoltre far sì che eventuali modalità alternative rispetto a quelle proposte nelle presenti Linee guida di espressione del consenso online siano realizzate in modo tale da rendere inequivoco anche per l'utente l'effetto della propria azione, equivalente alla manifestazione del consenso stesso. Ciò, allo scopo di limitare l'incidenza dei c.d. "falsi positivi", ossia di erronee interpretazioni di azioni casuali come espressioni consapevoli della volontà dell'utente.

Qualora invece, nel caso concreto, all'azione dell'utente non corrisponda alcun evento informatico inequivoco, documentabile e dotato delle menzionate caratteristiche anche sotto il profilo della consapevolezza per lo stesso utente, allora in nessun modo sarà possibile attribuire a tale azione la validità del consenso ai sensi della normativa vigente.

Ulteriori chiarimenti appaiono opportuni con riferimento al cd. cookie wall, intendendosi con tale espressione un meccanismo vincolante (cd. "take it or leave it"), nel quale l'utente venga cioè obbligato, senza alternativa, ad esprimere il proprio consenso alla ricezione di cookie ovvero altri strumenti di tracciamento, pena l'impossibilità di accedere al sito.

Tale meccanismo, non consentendo di qualificare l'eventuale consenso così ottenuto come conforme alle caratteristiche imposte dal Regolamento, e segnatamente al suo art. 4, punto 11 con particolare riferimento al requisito della "libertà" del consenso, è da ritenersi illecito, salva

l'ipotesi da verificare caso per caso nella quale il titolare del sito offra all'interessato la possibilità di accedere ad un contenuto o a un servizio equivalenti senza prestare il proprio consenso all'installazione e all'uso di cookie o altri strumenti di tracciamento.

E ciò alla irrinunciabile condizione della conformità dell'alternativa proposta ai principi del Regolamento codificati al suo art. 5, paragrafo 1, ed innanzitutto a quello di cui alla lettera a), che esige che i dati personali siano trattati in modo lecito, corretto e trasparente (principio di "liceità, correttezza e trasparenza"); in difetto, il cookie wall non potrà essere reputato in linea con la disciplina vigente.

6.2 La reiterazione della richiesta di consenso in presenza di una precedente mancata prestazione dello stesso

Ancora con riferimento alle modalità di acquisizione del consenso, l'osservazione del comportamento dei siti web e le segnalazioni pervenute hanno evidenziato l'ulteriore problematica della spesso ridondante ed invasiva riproposizione, da parte dei gestori dei siti web, del meccanismo basato sulla presentazione del banner ad ogni nuovo accesso dell'utente al medesimo sito anche quando quest'ultimo abbia liberamente scelto. Una implementazione che, se da un lato compromette la fluidità della user experience, non trova ragione negli obblighi di legge ed ha contribuito sin qui ad una probabile sottovalutazione del valore del contenuto con esso proposto.

L'eccessiva riproposizione del banner ai fini dell'acquisizione del consenso, laddove l'utente l'abbia in precedenza negato, appare suscettibile di lederne la libertà inducendolo a prestarlo pur di proseguire nella navigazione libero dalla comparsa del banner contenente l'informativa breve e la richiesta di prestazione del consenso.

In tale contesto, quindi, nel caso in cui l'utente mantenga le impostazioni di default e dunque non acconsenta all'impiego di cookie o altri strumenti di tracciamento, così come nel caso in cui abbia acconsentito solo all'impiego di alcuni cookie o altri strumenti di tracciamento, tale scelta dovrà essere debitamente registrata e la prestazione del consenso non più nuovamente sollecitata se non quando ricorra uno dei seguenti casi:

- quando mutino significativamente una o più condizioni del trattamento e dunque il banner assolva anche ad una specifica e necessaria finalità informativa proprio in ordine alle modifiche intervenute, come nel caso in cui mutino le "terze parti";

- quando sia impossibile, per il gestore del sito web, avere contezza del fatto che un cookie sia stato già in precedenza memorizzato sul dispositivo per essere nuovamente trasmesso, in occasione di una successiva visita del medesimo utente, al sito che lo ha generato (ad esempio nel caso in cui l'utente scelga di cancellare i cookie legittimamente installati nel proprio dispositivo senza che il titolare abbia modo, dunque, di tenere traccia della volontà di mantenere le impostazioni di default e dunque di proseguire la navigazione senza essere tracciati);

- quando siano trascorsi almeno 6 mesi dalla precedente presentazione del banner.

7. La privacy by design e by default in relazione ai cookie ed agli altri strumenti di tracciamento

7.1 Il meccanismo di acquisizione del consenso

È opinione del Garante che il meccanismo di acquisizione del consenso online tramite presentazione di un banner, come lo si è analiticamente descritto nel provvedimento del maggio 2014, mantenga, ad oggi, una sua sostanziale validità. È tuttavia necessario, anche in questo

caso, valutare l'opportunità di aggiornamenti o migliorie alla luce del mutato assetto normativo.

Al riguardo, occorre prendere in considerazione la portata innovativa del Regolamento e i nuovi equilibri che esso tratteggia nelle relazioni tra titolare e interessato con specifico riferimento al suo art. 25, il quale dispone, al secondo paragrafo, che "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità …".

In adempimento di tale obbligo, di carattere generale poiché applicabile a qualsiasi trattamento di dati, il titolare dovrà garantire che, per impostazione predefinita, siano trattati solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non eccedano il minimo necessario per il conseguimento delle finalità perseguite, in modo che l'utilizzo di informazioni per l'accesso ad un sito sia inizialmente limitato al minimo indispensabile per consentirne la fruizione e che sia rimesso interamente all'interessato un effettivo, concreto potere di scelta in ordine alla possibilità di consentire o meno un utilizzo eventualmente più ampio dei suoi dati.

Il rispetto di tali regole impone dunque che, per impostazione predefinita, al momento del primo accesso dell'utente a un sito web, nessun cookie o altro strumento diverso da quelli tecnici venga posizionato all'interno del suo dispositivo, né che venga utilizzata alcuna altra tecnica attiva o passiva di tracciamento.

Questo risultato costituisce un obbligo espressamente codificato il cui mancato adempimento è sanzionabile ai sensi del Regolamento. Nella propria autonomia imprenditoriale e in ossequio all'accountability, ciascun titolare può naturalmente adottare le modalità ritenute più idonee per assicurarne il rispetto.

Tuttavia, e considerato pure che occorre assicurare anche la libertà di scelta di chi invece intenda accettare di essere profilato, il Garante suggerisce l'adozione dello specifico modello, di seguito illustrato, da reputarsi in linea con i menzionati obblighi. Qualora i gestori dei siti web decidano di conformarvisi, dovranno implementare un meccanismo in base al quale l'utente, accedendo per la prima volta alla home page (o ad altra pagina) del sito web, visualizzi immediatamente un'area o banner le cui dimensioni siano, al tempo stesso, sufficienti da costituire una percettibile discontinuità nella fruizione dei contenuti della pagina web che sta visitando, ma anche tali da evitare il rischio che l'utente possa far ricorso a comandi e dunque compiere scelte indesiderate o inconsapevoli; con l'effetto che l'adeguatezza e la congruità delle dimensioni del banner dovranno essere valutate anche in relazione ai diversi dispositivi di possibile utilizzo da parte dell'interessato.

Tale banner dovrà essere parte integrante di un meccanismo che, pur non impedendo il mantenimento delle impostazioni di default, permetta anche l'eventuale espressione di una azione positiva nella quale deve sostanziarsi la manifestazione del consenso dell'interessato.

Qualora l'utente scegliesse, com'è nella sua piena disponibilità, di mantenere quelle impostazioni di default e dunque di non prestare il proprio consenso al posizionamento dei cookie o all'impiego di altre tecniche di tracciamento, dovrebbe dunque limitarsi a chiudere il banner mediante selezione dell'apposito comando usualmente utilizzato a tale scopo, cioè quello contraddistinto da una X posizionata di regola, e secondo prassi consolidata, in alto a destra e all'interno del banner medesimo, senza essere costretto ad accedere ad altre aree o pagine a ciò appositamente dedicate. Tale comando dovrà avere una evidenza grafica pari a quella degli ulteriori comandi o pulsanti negoziali idonei ad esprimere le altre scelte nella disponibilità dell'utente, di cui si dirà in appresso. Le modalità di prosecuzione nella navigazione senza prestare alcun consenso

dovranno, in altre parole, essere immediate, usabili e accessibili quanto quelle previste per la prestazione del consenso.

Mediante il ricorso a questo meccanismo si garantirebbe che, appunto by default, l'interessato che non intenda esprimere il proprio consenso non sia in alcun modo tracciato o profilato conseguendo, al tempo stesso, l'ulteriore risultato di generare un evento informatico riconoscibile e registrabile da parte del titolare. Esso, esprimendo la volontà dell'interessato di non prestare il proprio consenso all'utilizzo di cookie o altri strumenti di tracciamento diversi da quelli tecnici, impedirebbe al sito la reiterazione della presentazione del banner in occasione di successivi accessi dell'utente, fatte salve le eccezioni descritte al paragrafo precedente e, comunque, per un periodo di tempo non inferiore a 6 mesi.

In altri termini, il consenso potrà intendersi come validamente prestato soltanto se sarà conseguenza di un intervento attivo e consapevole dell'utente, opportunamente riscontrabile e dimostrabile, che consenta di qualificarlo come in linea con tutti quei requisiti (libero, informato, inequivoco e specifico, cioè espresso in relazione a ciascuna diversa finalità del trattamento) richiesti dal Regolamento.

Tale banner dovrà allora contenere, oltre alla X in alto a destra di cui è stata già illustrata la funzione, almeno le seguenti indicazioni ed opzioni:

i) l'avvertenza che la chiusura del banner mediante selezione dell'apposito comando contraddistinto dalla X posta al suo interno, in alto a destra, comporta il permanere delle impostazioni di default e dunque la continuazione della navigazione in assenza di cookie o altri strumenti di tracciamento diversi da quelli tecnici;

ii) una informativa minima relativa al fatto che il sito utilizza – se così è ovviamente - cookie o altri strumenti tecnici e potrà, esclusivamente previa acquisizione del consenso dell'utente da prestarsi con modalità da indicarsi nella medesima informativa breve (cfr. punto iv che segue), utilizzare anche cookie di profilazione o altri strumenti di tracciamento al fine di inviare messaggi pubblicitari ovvero di modulare la fornitura del servizio in modo personalizzato al di là di quanto strettamente necessario alla sua erogazione, cioè in linea con le preferenze manifestate dall'utente stesso nell'ambito dell'utilizzo delle funzionalità e della navigazione in rete e/o allo scopo di effettuare analisi e monitoraggio dei comportamenti dei visitatori di siti web;

iii) il link alla privacy policy, ovvero ad una informativa estesa posizionata in un second layer – che sia accessibile con un solo click anche tramite un ulteriore link posizionato nel footer di qualsiasi pagina del dominio cui l'utente accede - ove vengano fornite in maniera chiara e completa almeno tutte le indicazioni di cui agli artt. 12 e 13 del Regolamento, anche con riguardo ai predetti cookie o altri strumenti tecnici (cfr., al riguardo, il successivo paragrafo 8);

iv) un comando attraverso il quale sia possibile esprimere il proprio consenso accettando il posizionamento di tutti i cookie o l'impiego di eventuali altri strumenti di tracciamento;

v) il link ad una ulteriore area dedicata nella quale sia possibile selezionare, in modo analitico, soltanto le funzionalità, i soggetti cd. terze parti - il cui elenco deve essere tenuto costantemente aggiornato, siano essi raggiungibili tramite specifici link ovvero anche per il tramite del link al sito web di un soggetto intermediario che li rappresenti - ed i cookie, anche eventualmente raggruppati per categorie omogenee, al cui utilizzo l'utente scelga di acconsentire.

In quest'ultima ipotesi, quando cioè i cookie siano raggruppati per categorie omogenee, qualora si

verificassero successive modifiche nel novero delle terze parti corrispondenti ai link posizionati in questa area e dunque ulteriori soggetti terze parti venissero aggiunti alla lista, è rimessa alla prima parte, cioè al gestore del sito, la loro accurata selezione, come pure la necessaria attività di vigilanza per assicurare che l'ingresso di tali soggetti ed il trattamento che ne discende permanga in linea con il raggruppamento per categorie omogenee come già effettuato.

Anche in questo caso, il rispetto degli obblighi di privacy by default impone che le possibili scelte granulari siano inizialmente tutte preimpostate sul diniego all'installazione dei cookie, e che pertanto l'utente possa, esclusivamente, accettarne, anche appunto in modo granulare, il posizionamento.

Nell'eventualità in cui sia prevista la sola presenza di cookie tecnici o altri strumenti analoghi, di essi potrà essere data informazione nella homepage o nell'informativa generale senza l'esigenza di apporre specifici banner da rimuovere a cura dell'utente.

Queste premesse consentono anche di chiarire possibili fraintendimenti nel significato da attribuire all'azione dell'utente in relazione alla specifica configurazione dei pulsanti e dei colori utilizzati dai publisher, sinora di non univoca interpretazione. Basti, al riguardo, ribadire che, a prescindere dalla configurazione adottata, dai colori utilizzati per i pulsanti e in definitiva dalle modalità attuative prescelte, l'azione positiva nella disponibilità dell'utente al momento del primo accesso al sito dovrà comunque essere esclusivamente volta alla manifestazione del consenso (cd. opt-in) e non potrà mai riferirsi invece all'espressione di un diniego (cd. opt-out).

A tale riguardo, il Garante torna a sottolineare tuttavia l'importanza di avviare nelle sedi più opportune e tra tutti i soggetti interessati (accademia, industria, associazioni di categoria, decisori, stakeholder etc.) una riflessione circa la necessità dell'adozione di una codifica standardizzata relativa alla tipologia dei comandi, dei colori e delle funzioni da implementare all'interno dei siti web per conseguire la più ampia uniformità, a tutto vantaggio della trasparenza, della chiarezza e dunque anche della migliore conformità alle regole; tale esigenza, che sulla base dei contributi pervenuti nell'ambito della consultazione pubblica risulta essere unanimemente avvertita e condivisa, non ha tuttavia sin qui trovato delle proposte concrete idonee al conseguimento dello scopo.

Gli utenti, naturalmente, dovranno essere posti in condizione di modificare le scelte compiute – sia in termini negativi che in termini positivi e dunque prestando un consenso negato o revocando un consenso prestato – in ogni momento e ciò in maniera semplice, immediata e intuitiva attraverso un'apposita area da rendere accessibile attraverso un link da posizionarsi nel footer del sito e che ne renda esplicita la funzionalità attraverso l'indicazione di "rivedi le tue scelte sui cookie" o analoga.

Resta, peraltro, inteso che in ogni ipotesi di riproposizione del banner contenente l'informativa breve e le opzioni di scelta dell'utente, così come laddove l'utente modifichi le scelte originariamente compiute in conformità al periodo precedente, le scelte negoziali compiute in occasione degli accessi successivi dovranno sovrascrivere e superare le precedenti ed essere, dunque, considerate come modifica delle precedenti opzioni anche in questo caso, indifferentemente, in termini di prestazione di un consenso originariamente negato o di revoca di un consenso precedentemente prestato.

Per assicurare che gli utenti non siano influenzati ovvero penalizzati da scelte di design che inducano a preferire una opzione anziché l'altra, si sottolinea inoltre l'esigenza dell'utilizzo di comandi e di caratteri di uguali dimensioni, enfasi e colori, che siano ugualmente facili da visionare e utilizzare.

Al fine di rendere concretamente azionabile tale possibilità di mutare avviso e dunque effettiva la

disponibilità per l'utente della espressione libera della propria volontà, il Garante suggerisce allora l'adozione di una buona prassi, individuata attraverso l'esame dei contributi pervenuti nel corso della consultazione pubblica. Ci si riferisce al posizionamento in ciascuna pagina del dominio, eventualmente pure accanto al link all'area dedicata alle scelte, di un segno grafico, una icona o altro accorgimento tecnico che indichi, anche in modo essenziale, lo stato dei consensi in precedenza resi dall'utente consentendone, dunque, in ogni momento l'eventuale modifica o aggiornamento.

Per realizzare la memorizzazione delle azioni e delle scelte, anche di dettaglio, rimesse all'interessato (mantenimento delle impostazioni di default, espressione, anche granulare, del consenso ovvero revoca del consenso precedentemente espresso mediante ripristino delle impostazioni di default), il gestore del sito web potrebbe avvalersi o di appositi cookie tecnici (in tal senso, si veda anche il considerando 25 della direttiva 2002/58/CE) o anche di ulteriori modalità che la tecnologia dovesse rendere disponibili, la cui individuazione rientra nell'autonomia imprenditoriale e nell'accountability del titolare, adattando opportunamente la propria condotta in modo da tenere comunque costantemente aggiornata la documentazione delle scelte compiute dall'interessato.

Resta in ogni caso impregiudicata la possibilità per i titolari di adottare eventualmente anche diverse modalità di raccolta del consenso, ad esempio con riferimento a quegli utenti che accedano ai relativi servizi mediante uso di credenziali di autenticazione o di accesso e per i quali dunque, fin dal momento della creazione dell'account, si porrebbe un naturale momento di discontinuità nella navigazione idoneo, per il titolare, all'assolvimento degli obblighi che interessano l'impiego di cookie e degli altri strumenti di tracciamento; con l'avvertenza che a questi specifici utenti, cd. autenticati, dovrà inoltre essere consentito di scegliere consapevolmente - menzionando dunque tale possibilità pure nell'informativa resa - se accettare la possibilità che il tracciamento che li riguarda venga effettuato anche attraverso l'analisi incrociata dei comportamenti tenuti tramite l'utilizzo di diversi device.

7.2 I cookie analytics di prima parte e delle cd. terze parti

I cookie possono anche essere utilizzati, tra l'altro, per valutare l'efficacia di un servizio della società dell'informazione fornito da un publisher, per la progettazione di un sito web o per contribuire a misurarne il "traffico", cioè il numero di visitatori anche eventualmente ripartiti per area geografica, fascia oraria della connessione o altre caratteristiche.

L'Autorità ha affermato, nel provvedimento del maggio 2014, che tali identificativi, definiti cookie analytics, possono essere ricompresi nella categoria di quelli tecnici, e come tali essere utilizzati in assenza della previa acquisizione del consenso dell'interessato, al verificarsi di determinate condizioni. Anche in questo caso, l'entrata in vigore del Regolamento impone un ripensamento critico delle condizioni identificate allora, nonché una più specifica definizione delle misure oggi idonee all'applicazione della richiamata esenzione.

Si impone, in primo luogo, la necessità di individuare soluzioni di maggior tutela dell'interessato attraverso l'impiego di misure in linea con le disposizioni dell'art. 25, paragrafo 1, del Regolamento in materia di privacy by design, tali da "attuare in modo efficace i principi di protezione dei dati".

In questa prospettiva, il Garante reputa che, nel caso di specie, tale obiettivo debba essere conseguito attraverso il ricorso a misure di minimizzazione del dato che riducano significativamente il potere identificativo dei cookie analytics, qualora il loro utilizzo avvenga ad opera di "terze parti".

Affinché i cookie analytics siano equiparati ai tecnici è, in altri termini, indispensabile precludere la possibilità che si pervenga, mediante il loro utilizzo, alla diretta individuazione dell'interessato (cd.

single out), il che equivale impedire l'impiego di cookie analytics che, per le loro caratteristiche, possano risultare identificatori diretti ed univoci.

La struttura del cookie analytics dovrà allora prevedere la possibilità che lo stesso cookie sia riferibile non soltanto ad uno, bensì a più dispositivi, in modo da creare una ragionevole incertezza sull'identità informatica del soggetto che lo riceve. Di regola questo effetto si ottiene mascherando opportune porzioni dell'indirizzo IP all'interno del cookie.

Tenuto conto della rappresentazione degli indirizzi IP versione 4 (IPv4) a 32 bit, che sono usualmente rappresentati e utilizzati come sequenza di quattro numeri decimali compresi tra 0 e 255 separati da un punto, una delle misure implementabili al fine di beneficiare dell'esenzione consiste nel mascheramento almeno della quarta componente dell'indirizzo, opzione che introduce una incertezza nell'attribuzione del cookie ad uno specifico interessato pari a 1/256 (circa 0,4%).

Analoghe procedure dovrebbero essere adottate in riferimento agli indirizzi IP versione 6 (IPv6), che hanno una differente struttura e uno spazio di indirizzamento enormemente superiore (essendo costituiti da numeri binari rappresentati con 128 bit).

Il Garante sottolinea, inoltre, la necessità che l'uso dei cookie analytics sia limitato unicamente alla produzione di statistiche aggregate e che essi vengano utilizzati in relazione ad un singolo sito o una sola applicazione mobile, in modo da non consentire il tracciamento della navigazione della persona che utilizza applicazioni diverse o naviga in siti web diversi.

Resta inteso pertanto che i soggetti terzi, che forniscono al publisher il servizio di web measurement, non dovranno comunque combinare i dati, anche così minimizzati, con altre elaborazioni (file dei clienti o statistiche di visite ad altri siti, ad esempio) nè trasmetterli a loro volta ad ulteriori terzi, pena l'inaccettabile incremento dei rischi di identificazione dell'utente; tranne il caso in cui la produzione di statistiche da loro effettuata con i dati minimizzati interessi più domini, siti web o app riconducibili al medesimo publisher o gruppo imprenditoriale.

È tuttavia possibile reputare lecito, anche in assenza dell'adozione delle prescritte misure di minimizzazione, il ricorso ad analisi statistiche relative a più domini, siti web o app riconducibili al medesimo titolare purché questi proceda in proprio all'elaborazione statistica, senza in ogni caso che tali analisi si risolvano in una attività che, travalicando i confini di un mero conteggio statistico, assuma in realtà le caratteristiche di una elaborazione volta all'assunzione di decisioni di natura commerciale.

8. Le novità in materia di informativa

8.1 Le informazioni da rendere in conformità al Regolamento

Da ultimo, il Garante intende illustrare alcuni miglioramenti che i titolari potranno adottare al fine di rendere agli utenti una informativa conforme ai rinnovati requisiti di trasparenza imposti dagli articoli 12 e 13 del Regolamento, compresa l'indicazione circa gli eventuali altri soggetti destinatari dei dati personali ed i tempi di conservazione delle informazioni acquisite.

È inoltre necessario fornire informazioni su come le persone fisiche possono esercitare tutti i diritti previsti dal Regolamento, incluso quello di avanzare una richiesta di accesso e di proporre un reclamo a un'Autorità di controllo.

In aggiunta a quanto stabilito nel provvedimento sui cookie del maggio 2014, e nel confermare la logica di semplificazione cui le sue indicazioni sono improntate, si ritiene inoltre che l'informativa, oltre che multilayer, e cioè dislocata su più livelli, possa ad oggi essere resa, eventualmente in relazione a specifiche necessità, anche per il tramite di più canali e modalità (cd. multichannel), in

modo da sfruttare al massimo più dinamici e meno tradizionali ulteriori punti di contatto tra il titolare e gli interessati.

Si pensi, ad esempio, al sempre più diffuso ricorso a canali video, a pop-up informativi, a interazioni vocali, ad assistenti virtuali, all'impiego del telefono, al ricorso a chatbot, etc.

Sarà allora onere del titolare, cui è rimessa la scelta in ordine alla modalità ovvero all'impiego combinato delle modalità ritenute più idonee, verificare la corrispondenza del sistema implementato, specie in termini di completezza, chiarezza espositiva, efficacia e fruibilità, con i requisiti imposti dal Regolamento.

Allo stesso modo, sarà onere del titolare adottare ogni più opportuno accorgimento affinché le informazioni contenute nel banner siano fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari, in linea con quanto previso dalla legge 9 gennaio 2004, n. 4 (come modificata, da ultimo, dal d.l. 16 luglio 2020, n. 76, convertito in legge, con modificazioni, dalla legge 11 settembre 2020, n. 120).

8.2 La necessità di una integrazione delle informazioni da comunicare agli utenti

La pratica operativa degli ultimi anni ha evidenziato come il sistema difetti di un elemento di cruciale rilievo, specie a fini di enforcement.

Ci si riferisce al fatto che non esiste ancora, ad oggi, un sistema universalmente accettato di codifica semantica dei cookie e degli altri strumenti di tracciamento che consenta di distinguere oggettivamente, ad esempio, quelli tecnici dagli analytics o da quelli di profilazione, se non basandosi sulle indicazioni rese dal titolare stesso nella privacy policy.

È stato riscontrato, inoltre, che le interrogazioni e le verifiche circa il posizionamento di cookie da parte di uno specifico sito web possono avere esiti diversi a seconda del browser considerato.

In tale situazione, e con l'auspicio che si addivenga in tempi rapidi ad una codifica di carattere generale, tanto più importante specie nell'attuale mondo connesso online, nel quale le distanze geografiche perdono rilevanza a fronte delle sempre più accentuate potenzialità della rete, il Garante intende richiamare i titolari che facciano impiego di tali strumenti alla necessità di rendere manifesti, mediante apposita, opportuna integrazione dell'informativa, almeno i criteri di codifica degli identificatori adottati da ciascuno. In alternativa, i titolari potranno valutare di posizionare tale codifica anche all'interno della privacy policy.

Tali criteri potranno, inoltre, a richiesta, costituire oggetto di comunicazione all'Autorità, quale strumento di ausilio alle attività di carattere istruttorio che saranno intraprese con riguardo al fenomeno in considerazione.

TUTTO CIÒ PREMESSO, IL GARANTE:

ai sensi dell'art. 154-bis, comma 1, lett. a), del Codice, delibera di adottare le presenti Linee guida affinché tutti i fornitori dei servizi della società dell'informazione di cui all'art. 1, paragrafo 1, punto (b) della Direttiva (EU) 2015/1535, nonché tutti i soggetti che comunque offrono ai propri utenti servizi online accessibili al pubblico attraverso reti di comunicazione elettronica o cui si riferiscano siti web che facciano impiego di cookie e/o altri strumenti di tracciamento, con specifico riguardo ai trattamenti di dati personali relativi all'utilizzo delle funzionalità offerte, tengano conto delle indicazioni e delle semplificazioni illustrate; segnatamente, per quanto concerne:

- il consenso preventivo degli utenti in relazione al trattamento, per finalità di tracciamento on line, delle informazioni che li riguardano, anche derivanti dall'uso di

cookie ed altri strumenti di tracciamento, ai sensi degli artt. 122 del Codice e 4, punto 11) e 7 del Regolamento (secondo i criteri e le modalità indicate ai paragrafi 6 e 7);

- il rispetto del diritto di revoca del consenso nei termini di cui all'art. 7.3 del Regolamento (secondo quanto indicato al paragrafo 7.1);

- il rispetto degli obblighi di privacy by design e by default di cui all'art. 25 del Regolamento anche per mezzo dell'adozione di misure di minimizzazione dei dati preliminarmente alla comunicazione ed al loro impiego ad opera delle cd. terze parti (secondo quanto indicato al paragrafo 7.2);

- l'informativa da rendere agli interessati ai sensi degli artt. 12 e 13 del Regolamento, con particolare riguardo all'indicazione dei criteri di codifica utilizzati da ciascun titolare per la classificazione dei cookie e degli altri strumenti di tracciamento che consenta di distinguere quelli tecnici dagli analytics o da quelli di profilazione (secondo quanto indicato al paragrafo 8 delle presenti Linee guida).

In considerazione della potenziale complessità di eventuali adeguamenti dei sistemi e dei trattamenti già in atto ai principi espressi dalle presenti Linee Guida, l'Autorità reputa congruo individuare un termine pari a 6 mesi dal momento della loro pubblicazione in Gazzetta Ufficiale entro il quale i soggetti tenuti dovranno conformarvisi; con l'avvertenza che i consensi già raccolti, purché conformi alle caratteristiche richieste dal Regolamento, potranno essere ritenuti validi a condizione che, al momento della loro acquisizione, siano stati registrati e siano dunque debitamente documentabili, anche mediante evidenze informatiche.

Si allega alle presenti Linee Guida una scheda di sintesi (all. 1) che ne costituisce parte integrante e sostanziale.

Si dispone la trasmissione di copia delle presenti Linee guida al Ministero della Giustizia-Ufficio pubblicazione leggi e decreti, per la loro pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 10 giugno 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL SEGRETARIO GENERALE
Mattei

NOTE

(1) V. considerando 32 del Regolamento e il raffronto tra l'art. 2, lettera h) della direttiva 95/46/Ce e l'art. 4, punto 11) del Regolamento).

(2) Così la Corte di Giustizia, che nella sentenza Wirtschaftsakademie (C-210/16 del 5 giugno 2018) ha applicato la direttiva 95/46 nonostante il caso si riferisse a operazioni di trattamento rientranti nell'ambito di applicazione materiale della direttiva ePrivacy; lo stesso è accaduto nella sentenza resa nel caso Fashion ID (C-40/17 del 29 luglio 2019).

(3) In senso conforme, con specifico riguardo alle interrelazioni tra le due discipline, si veda anche il parere dell'EDPB n. 5/2019 del 12 marzo 2019, richiamato in premessa.

(4) "Based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it" (cfr. punto 86).

_____

Guidelines on the use of cookies and other tracking tools – 10 June 2021
(Published in the Official Journal of the Italian Republic No 163 of 9 July 2021)

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In today's meeting, attended by Prof. Pasquale Stanzione, President; Prof. Ginevra Cerrina Feroni, Vice-President; Dott. Agostino Ghiglia and Avv. Guido Scorza, Members, and Dott. Fabio Mattei, Secretary General;

Having regard to directive 2002/21/EC of 7 March 2002, of the European Parliament and of the Council, on a common regulatory framework for electronic communications networks and services ('Framework Directive') as amended and supplemented thereafter;

Having regard to directive 2002/58/EC of 12 July 2002, of the European Parliament and of the Council, on the processing of personal data and the protection of privacy in the electronic communications sector ('E-privacy Directive') as amended by directive 2009/136/EC of 25 November 2009 of the European Parliament and of the Council;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to the Personal Data Protection Code (legislative decree No 196 of 30 June 2003) as amended by legislative decree No 101 of 10 August 2018 containing provisions to adapt the national legal system to the said Regulation;

Having regard to legislative decree No 29 of 28 May 2012 containing 'Amendments to legislative decree No 196 of 30 June 2003 containing the personal data protection Code to transpose Directive 2009/136/EC on the processing of personal data and the protection of privacy in the electronic communications sector and Directive 2009/140/EC on electronic communications networks and services and implementing Regulation (EC) 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws';

Having regard to Opinion 4/2012 by the Article 29 Working Party (hereinafter 'WP29') concerning cookie consent exemption as adopted on 7 June 2012, and to the Working Document 2/2013 by the said WP29 providing guidance on obtaining consent for cookies as adopted on 2 October 2013, and to the WP29 Guidelines on consent under Regulation (EU) 2016/679 as adopted on 10 April 2018, endorsed by the European Data Protection Board (EDPB) on 25 May 2018, and replaced by Guidelines 5/2020 on consent under Regulation 2016/679 adopted on 4 May 2020;

Having regard to the EDPB Opinion 05/2019 on the interactions between the e-privacy directive and the Regulation, with particular regard to the competences, powers and tasks of supervisory authorities;

Having regard to the Garante's decision No 229 of 8 May 2014 concerning 'Determination of simplified arrangements for information notices and obtaining consent for the use of cookies' as published in the Official Journal of the Italian Republic of 3 June 2014;

Having regard to the FAQs on information and consent for the use of cookies of 3 December 2014 and to the 'Clarifications on the implementation of rules concerning cookies' of 5 June 2015 as published by the Garante on its website at www.garanteprivacy.it;

Having regard to the Garante's decision No 161 of 19 March 2015 concerning 'Guidelines on the processing of personal data for online profiling purposes' as published in the Official Journal of the Italian Republic of 6 May 2015;

Having regard to the resolution by the Garante No 255 of 26 November 2020 (web document No 9498472) whereby 'Draft guidelines on the use of cookies and other tracking tools' were adopted (Annex 1, web document No 9501061) along with the respective executive summary (Annex 2, web document No 9501097) and a public consultation was launched on the measures set out therein by publishing the relevant notice in the Official Journal of the Italian Republic of 11 December 2020;

Having regard to the outcome of the said public consultation, which was intended to 'gather comments and proposals regarding the said Guidelines';

Having regard, in particular, to the contributions submitted within the 30-day deadline by several trade associations, operators and entrepreneurial entities, consumer associations, academia representatives and individuals;

Having regard to the documentation on file;

Having regard to the considerations submitted by the Office as reported by the Secretary General pursuant to Article 15 of the Garante's Internal Regulations No 1/2000 of 28 June 2000;

Acting on the report submitted by Avv. Guido Scorza;

WHEREAS

1. Preliminary remarks

These guidelines are intended in the first place to provide an overview of the law applicable to reading and writing operations within a user's terminal, with specific reference to the use of cookies and other tracking tools. Secondly, they are intended to specify, in this regard, the appropriate arrangements for the provision of information and for obtaining the data subjects' consent online, where necessary, in the light of the full-fledged application of Regulation (EU) 2016/679 (hereinafter 'Regulation').

The relevant legal framework includes, to date, both the provisions of Directive 2002/58/EC (so-called ePrivacy Directive), as amended and transposed into national law by Section 122 of Legislative Decree No 196 of 30 June 2003 (hereinafter the 'Code'), and the Regulation. The latter applies as regards specifically the concept of consent referred to in Articles 4 (11) and 7 and recital 32, as last interpreted by the WP29 Guidelines adopted on 10 April 2018 and endorsed by the European Data Protection Board (hereinafter the 'EDPB') on 25 May 2018 and subsequently replaced by the Guidelines No 05/2020 on consent under Regulation 2016/679, which were

adopted on 4 May 2020.

In this context, the Garante already adopted a Decision (No 229 of 8 May 2014) aimed at 'identifying simplified arrangements for providing online information to users on the cookies stored on their terminals by visited websites' as well as 'providing appropriate guidance on how to obtain the users' consent, where required by the law'. Such guidance now needs to be supplemented and detailed further, in particular with reference to certain specific aspects. A table summarizing the measures set out in the preceding and the current guidelines is attached in order to facilitate implementation by controllers of the relevant regulatory framework as outlined in both sets of guidelines – i.e., the 2014 and the current ones.

On the one hand, it should be borne in mind that the Regulation, as stated in its Article 95, 'shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communications networks in the Union, in relation to matters for which they are subject to specific obligations with the same objective laid down in Directive 2002/58/EC', which expressly provides under Article 1 (2) that 'the provisions of this Directive particularise and complement [Regulation (EU) 2016/679] …'.

On the other hand, one should not fail to take into due account that the Regulation is intended to expand and enhance the power of the individual to organise and control the processing of his or her personal information, in particular by supplementing the definition of consent contained in Directive 95/46/EC; by clarifying that the data subject's indication of consent to the processing of his or her personal data must be not only free, specific and informed, as was already the case with the Directive, but also 'unambiguous'(1); and by requiring that the concrete, effective implementation of data protection principles is achieved by design and by default.

The need for further guidance by the Garante is grounded in the time that has elapsed, the regulatory changes that have taken place in the meantime, and the monitoring that has been carried out by the Authority on the practical (at times incorrect) implementation of the rules at issue also through the numerous complaints, alerts and requests for opinions it has received - particularly in view of the effects that can be observed on navigation experience, on the rights and safeguards for data subjects as well as on the activities of electronic communications services companies and providers. Reference should also be made to the ever-increasing spread of new technologies featuring a growing level of potential pervasiveness.

Finally, account should be taken of the evolution in the behavior of network users themselves, who are increasingly oriented towards the multiplication of their digital identities as resulting from access to a number of available services and functions and, in the first place, social networks. This poses the risk that personal information being processed will be collected precisely by cross-checking data relating to the use of different functionalities and services that can be accessed by way of several terminal devices (so-called enrichment), thereby creating increasingly specific and detailed profiles. Accordingly, there is a need for an enhanced framework of safeguards that are more geared towards fostering and enforcing control over personal information undergoing processing and, ultimately, individual self-determination.

2. The function of cookies

Recital 30 of the Regulation expressly states that 'Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.'

Cookies are, as a rule, text strings that the websites visited by the user (so-called ‘publisher’ or ‘first party’ websites) or else different websites or web servers (so-called ‘third parties’) place and store within a terminal device in the user’s possession — whether directly as is the case with publisher websites, or indirectly as is the case with ‘third parties’, i.e. through the intermediation of the publisher websites.

The terminal devices referred to include, for example, a computer, a tablet, a smartphone, or any other device capable of storing information. In this respect, reference should also be made - already today, and even more so in the future – to IoT (Internet of Things) devices, which are designed to connect both to the network and to one another so as to provide services of various kinds, not necessarily limited to communication.

Software for browsing the internet and operating these devices can store cookies and then transmit them back to the sites that generated them on the occasion of a subsequent visit by the user, thus keeping track of that user’s previous interaction with one or more websites.

Information encoded in cookies may include personal data, such as an IP address, a username, a unique identifier or an email address, but it may also include non-personal data such as language settings or information on the type of device a person is using to navigate within the website.

Cookies can therefore perform important as well as diverse functions, including session monitoring, the storage of specific server access information related to user configuration, facilitating the use of online content, etc. For example, they can be used to keep track of the items in an online shopping basket or the information used to fill in a computer form.

On the one hand, it is through cookies that it is possible, inter alia, to allow web pages to upload more quickly as well as to route information on a network — i.e., to meet requirements that are closely linked to the operation of websites as such; on the other hand, it is still through cookies that behavioural advertising can be conveyed and the effectiveness of such advertising gauged or the services offered can be customized as for their nature and mechanisms to the user’s monitored behaviour.

3. Other tracking tools

The same objective can also be achieved by means of other tools, which can be classed on the whole as either ‘active identifiers’ – including cookies - or ‘passive identifiers’ - the latter being termed so on account of their merely observational role - which enable processing activities similar to those referred to above.

The ‘passive’ tools include fingerprinting, - i.e., a technology to identify the user’s device by collecting all or part of the information on the specific user-selected configuration of that device. This technique can be used to achieve the same profiling purposes, including the display of customised behavioural advertising and the analysis and monitoring of the behaviour of website visitors as well as to customize nature and mechanisms of the offered services to the behavior of a monitored user. For these reasons, fingerprinting and other tracking tools must be included in the scope of these Guidelines.

However, there is a significant difference to be highlighted between the use of an active technique such as that related to cookies and a passive one such as fingerprinting.

Indeed, in the former case users who do not wish to be profiled are able to refuse their consent or can avail themselves of the legal safeguards applying to the exercise of the rights provided for in the Regulation, but they can also rely practically on the possibility of directly removing the cookies stored on their own devices.

Conversely, with fingerprinting and any other ‘passive’ identifier the user does not have tools that can be relied on independently, since he or she must necessarily have recourse to the controller’s support. That is so because the controller uses a reading technique that does not require the storage of information within the user’s device, as it only envisages observing the configurations applying to that specific user and making him or her identifiable; the outcome is ultimately a ‘profile’ that remains in the controller’s sole possession, to which the data subject obviously has no free and direct access and of which the data subject might actually be totally unaware.

4. Categorization of cookies and other tracking tools

Cookies and, to a large extent, other tracking tools can have different features depending on their duration, i.e. on whether they are session or permanent cookies, as well as on the entity placing them - i.e., depending on whether the publisher acts directly or on behalf of a ‘third party’.

However, the rationale of the categorization made in the applicable legislation, which is also applicable to the relevant safeguards for individuals, envisages ultimately two broad categories:

- Technical cookies, which are used solely for the purpose of ‘carrying out the transmission of a communication over an electronic communications network, or to the extent strictly necessary for the provider of an information society service explicitly requested by the contracting party or user to provide that service’ (see Section 122 (1) of the Code);

- Profiling cookies, which are used to trace specific actions or recurring behavioral patterns in the use of the offered functionalities back to specific, identified or identifiable individuals for the purpose of grouping the different profiles within homogeneous, multi-sized clusters; this is aimed in turn to enable the controller to, inter alia, provide increasingly customized services beyond what is strictly necessary for the delivery of the given service and also send targeted advertising messages, i.e. messages that are in line with the preferences expressed by the user in the context of their web-browsing activities.

Similarly, the other identifiers can also be catalogued according to different criteria, of which the main one remains the purpose for which they are used – i.e., a ‘technical’ or ‘non-technical’ one. The latter category should be construed broadly, since the current legislation as intended to safeguard the confidentiality of electronic communications as well as of personal information (see below) is framed unquestionably in such a way as to generally ban any processing of data subjects’ information - except for certain situations that are set out in a stringent, highly specific manner and do not lend themselves to a looser interpretation based on analogy.

5. Applicable law

As for the use of cookies and other technical identifiers, the controller shall be only required to provide specific information, where appropriate as part of the general information notice, taking account of the functions pertaining to such cookies and within the limits and conditions referred to above; their use indeed falls within the scope of one of the legally permitted exemptions from the obligation to obtain the data subject’s consent. Conversely, cookies and other tracking tools serving purposes other than the technical ones may only be used after obtaining informed consent from the contracting party or user. This requirement stems from the provision that is still applicable to the specific case, namely Section 122 of the Code whereby

‘1. Storing information, or accessing information that is already stored, in the terminal equipment of a contracting party or user shall only be permitted on condition that the contracting party or user has given his consent after being informed in accordance with simplified arrangements. This shall be without prejudice to technical storage or access to stored information where they are aimed exclusively at carrying out the transmission of a

communication on an electronic communications network, or insofar as this is strictly necessary to the provider of an information society service that has been explicitly requested by the contracting party or user to provide the said service. In order to determine the simplified arrangements referred to herein, the Garante shall also take account of the proposals put forward by the nationally most representative consumer and industry associations involved in order to also ensure that the mechanisms implemented make the contracting party or user actually aware.

2. With a view to giving the consent referred to in paragraph 1 above, specific configurations of software or devices may be used that should be user-friendly as well as unambiguous vis-à-vis the contracting party or user.

2-a. Subject to the provisions made in paragraph 1 above, it shall be prohibited to use an electronic communications network in order to access information stored in the terminal equipment of a contracting party or user, store information, or monitor the operations performed by the user.'

This provision was introduced into national law following the transposition of the ePrivacy Directive, which was enacted prior to the date when the Regulation became fully operational. That Directive is still applicable to the specific area of data processing in the context of electronic communications exactly like the provisions of national law transposing it - see, in this regard, recital 173 of the Regulation whereby 'This Regulation should apply to all matters concerning the protection of fundamental rights and freedoms vis-à-vis the processing of personal data which are not subject to specific obligations with the same objective set out in Directive 2002/58/EC of the European Parliament and of the Council…' and Article 2, letter l), of the Framework Directive 2002/21/EC which includes the ePrivacy directive among the 'particular directives'.

Still, the entry into force of the Regulation makes it necessary to investigate, in the first place, the interactions between the two sets of rules. Except for the cases that are regulated exclusively and exhaustively by the ePrivacy Directive, many processing activities cannot but fall actually within the scope of application of both the Directive and the Regulation[(2)]. However, as regards the areas of potential overlap between the two, it should be clarified that the former specifies the latter since Article 1 (2) of the ePrivacy Directive clearly sets out that the provisions of the Directive particularise and complement those of the Regulation. Accordingly, whenever the Directive specifies provisions contained in the Regulation, it shall have to be applied as a lex specialis and prevail over the (more general) provisions contained in the Regulation. On the other hand, those provisions remain applicable to all cases that are not specifically regulated in the Directive, indeed they set out the general regulatory framework within which the requirements made in the Directive have to be placed.[(3)]

For example, the ePrivacy Directive is where the obligation to obtain consent as appropriate with a view to the use of cookies and other tracking tools is set out; however, the Regulation is where the specific requirements applying to consent are laid out and those requirements must be met in order to ensure that such consent is valid and compliant with the general rules.

One initial key conclusion can be drawn from the above analysis of the applicable legislation – namely, that the specific rules applicable to the specific processing situations do not envisage legal bases for such processing other than the data subject's consent or the fulfilment of any one of the conditions for derogating from the obligation to gather such consent as provided for in those rules. Accordingly, under no circumstances will it be permitted to rely on the controller's legitimate interest to justify the use of cookies or other tracking tools – contrary to what has been found in the course of the inquiries carried out into several web sites.

6. Obtaining consent online in the light of appropriate clarifications and new

recommendations

6.1. The so-called scrolling and cookie walls

The Garante considers that the reasoning underlying the determination of the technical arrangements to obtain online consent for tracking whether based on cookies or on other tools - as set out in the above-mentioned decision of May 2014 - remains valid in spite of the changed legal framework, which fosters accountability by controllers and requires the latter to act in accordance with this new paradigm (see Article 5 (2) of the Regulation) – whereby they are free to implement different approaches, where appropriate, to achieve compliance with the rules whilst safeguarding data subjects.

However, some clarifications are due regarding the use of so-called scrolling for the purpose of obtaining consent to the storage and use of cookies and other tracking tools as well as regarding the use of so-called cookie walls.

In this connection, it should first be recalled that recital 32 of the Regulation reads as follows: ‘Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.’

Furthermore, the EDPB recently clarified (Opinion No 5/2020 of 4 May 2020) that mere scrolling is never capable, in itself, of fully signalling the data subject’s intention to accept the reception of cookies other than technical ones within his or her terminal, and therefore does not amount per se to consent ‘under any circumstances’[(4)].

Obviously, the Garante shares the view outlined by the EDPB. Indeed, the mere scrolling down of the page bar is in itself unsuitable for the controller to obtain genuine consent to the storage and use of profiling cookies or other tracking tools.

However, one cannot rule out that scrolling can be part of the procedure to obtain consent and thus be one, rather than the only, component of a more complex process that allows the user to flag his or her informed choice unambiguously, i.e., the choice to consent to the use of such cookies or other tracking tools, in a manner that can be recorded and thus documented in line with the applicable legislation, by generating a precise pattern.

This conclusion is actually consistent with the current regulatory approach that leverages on accountability; therefore, similarly to what has been stated regarding the controller’s discretion in determining the most appropriate mechanisms to achieve compliance with data protection legislation, the Garante calls upon controllers to apply stringent criteria in assessing all possible solutions, including technical ones, that are suitable for being interpreted and recorded as the user’s explicit consent to the installation of cookies and/or the use of other tracking tools.

In order for consent to be obtained lawfully, a controller will also be required to make sure that any mechanisms for giving one’s consent online other than those proposed in these Guidelines are implemented in such a way as to make the effect produced by each action unambiguous for the

user as well – to the extent such action is tantamount to the provision of consent. This is intended to limit the occurrence of so-called ‘false positives’, i.e. random actions that are misinterpreted as indications of the user’s informed choice.

On the other hand, if the action performed by the user does not correspond in the specific case to any unambiguous, recordable IT event having the aforementioned characteristics - also in terms of that user’s awareness - then that action will in no way be liable to be considered valid consent within the meaning of the legislation in force.

Further clarification appears to be required with regard to the so-called cookie wall, which means a ‘take it or leave it’ mechanism in which the user is obliged to give his or her consent to the reception of cookies or other tracking tools - since failing to do so will prevent him or her from accessing the site.

Such a mechanism does not allow considering the consent obtained by its application as compliant with the requirements set out in the Regulation, in particular in Article 4 (11) thereof regarding ‘free’ consent; accordingly, it is to be regarded as unlawful except where the website controller provides the data subject with the option of accessing equivalent content or services without giving his or her consent to the storage and use of cookies or other tracking tools – which will have to be verified on a case-by-case basis.

At all events, an essential condition to be fulfilled is that the proposed alternative complies with the principles of the Regulation as laid down in Article 5 (1), and above all with letter (a) thereof whereby personal data shall be processed lawfully, fairly and in a transparent manner - that is to say, compliance with the principle of ‘lawfulness, fairness and transparency’ is paramount. Failing this, a cookie wall may not be deemed to be in line with the legislation in force.

6.2 The repetition of the request for consent after consent initially failed to be given

An additional issue that was brought to light regarding the methods for obtaining consent - based on several reports as well as on assessing the practices of websites - has to do with the often redundant, intrusive repetition by website operators of the presentation of the aforementioned banner each time the user accesses the given website including after that user has made his or her free choice. While jeopardizing the fluidity of the user experience, this approach is not justified by having regard to the legal requirements and is actually likely to have contributed to underrating the significance of the contents proposed in this manner.

The over-repetitive presentation of the banner to obtain the consent a user had previously withheld is liable to impact that user’s freedom by leading him or her to consent to the processing in order to continue browsing without being plagued by the appearance of a banner containing a short information notice and the request to give one’s consent. In such a situation, i.e. where a user sticks to the default configuration and does not consent to the use of cookies or other tracking tools as well as where a user has only consented to the installation of certain cookies or tracking tools, such choice will have to be duly recorded and the user’s consent will not be solicited any longer unless:

- one or more of the circumstances of the processing changes significantly, so that the banner also serves the specific as well as necessary purpose of informing exactly about the changes in question, e.g. regarding any of the ‘third parties’;

- it is impossible for the website operator to be aware that a cookie has already been stored on the device in order to be re-transmitted to the site that generated it, on the occasion of a subsequent visit by that user. This is the case, for instance, where the user chooses to delete the cookies lawfully stored in his/her device and the controller is unable to keep track

of the user's intention to stick to the default settings and accordingly to continue browsing without being tracked;

- at least six months have elapsed since the banner was last presented.

7. Privacy by design and by default as related to cookies and other tracking tools

7.1 The mechanism to obtain consent

It is the Garante's view that the mechanism for obtaining consent online via presentation of a banner as detailed in the May 2014 decision remains, to date, essentially valid. However, it is necessary, once again, to consider whether updates or improvements should be made in the light of the changed regulatory framework.

Account should be taken in this respect of the innovative scope of the Regulation and the new balance it envisages as for the relations between data controller and data subject by having regard to Article 25 thereof, whose paragraph 2 provides that 'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility (...)'.

In compliance with that obligation, which is general in nature since it applies to any processing of data, the controller shall ensure that, by default, only such personal data is processed as is necessary in relation to each specific purpose of the processing and that, in particular, the amount of collected data and the duration of their storage do not exceed the minimum necessary to achieve the intended purposes. Accordingly, the information used for accessing a website shall be initially limited to the minimum necessary to enable the data subject to use the services provided by the website and only the data subject shall be empowered effectively and factually to decide whether to allow his or her data to be used to a possibly larger extent.

Compliance with the above rules requires that, by default, no cookies or tools other than technical ones are placed on the user's device when that user first accesses a website, and that no other active or passive tracking technique is used at that time. This is an obligation expressly set out in the law and non-compliance carries penalties under the terms of the Regulation. Needless to say, freedom of enterprise coupled with the accountability principle entail that a controller is free to implement such arrangements as are considered most suited to achieve the said compliance.

However, given that it is also necessary to ensure the freedom of choice of those users who wish to agree to be profiled, the Garante suggests that website operators implement the approach described below which is considered to be in line with the aforementioned obligations. Where a website operator decides to follow this approach, it will have to deploy a mechanism whereby the user, on first accessing the website's home page (or another page), is immediately shown an area or a banner of a size that is sufficient to perceptibly interrupt the experience of browsing the contents of the relevant web page whilst preventing the risk for a user to activate commands and therefore make uninformed and/or unwanted choices. This means that in determining whether the banner size is adequate and appropriate account will have to also be taken of the different devices a data subject may be using. The said banner will have to be an integral part of a mechanism that, while not preventing the retention of default settings, also allows for an affirmative action such as to reflect the indication of the data subject's consent.

If the user chooses, as he or she is fully entitled to do, to keep the default settings and therefore not to give his or her consent to the storing of cookies or the use of other tracking techniques, that user should therefore simply close the banner by clicking on the command that is usually meant to

enable this action – i.e., the 'X' that is normally positioned according to well-received practice at the top right end of the banner area - without having to access other ad-hoc areas or pages. The command in question will have to be as visible as any other commands or buttons that may be used to flag other choices available to the users, which will be detailed below. In other words, the mechanism to enable continued browsing without giving any consent will have to be as user-friendly and accessible as the one in place for giving one's consent. This would ensure that, by default, the data subject who does not wish to express his or her consent is in no way tracked or profiled; at the same time, an IT event would be generated in this manner which can be recognized and recorded by the controller. Such IT event indicates the data subject's intention to not give his or her consent to the use of non-technical cookies or tracking tools and would thus prevent the website from repeatedly presenting the banner on the occasion of subsequent accesses by that user – subject to the exceptions listed in the foregoing paragraphs and in all cases for a period of not less than six months.

In other words, consent can only be considered to have been validly given if it is the result of an affirmative, conscious action by the user and if that action can be appropriately identified and demonstrated so that the consent in question can be ultimately considered to be in line with all the requirements set out in the Regulation. The latter provides that consent is to be free, informed, unambiguous and specific – i.e., specific to each different purpose of the processing.

Accordingly, the banner referred to above shall contain, in addition to the 'X' at its top right end, at least the following information and options:

(i) A warning to the effect that if the banner is closed by clicking on the 'X' at its top right end, the default settings are left unchanged and therefore browsing can continue without cookies or other tracking tools other than technical ones;

(ii) a minimal information notice to the effect that the website uses, if any, technical cookies or other technical tools and may, only after obtaining the user's consent according to the mechanism to be specified in this short information notice, also use profiling cookies or other tracking tools in order to send advertisements and/or customize its services beyond what is strictly necessary for the provision of those services, that is to say, in line with the preferences expressed by the user in the context of his/her use of functionalities and web browsing and/or for the purpose of analysing and monitoring the behaviour of website visitors;

(iii) a link to the privacy policy, or to a second-layer extended information notice – which should be one-click away through a link to be placed in the footer of any page of the domain accessed by the user - where at least all the information referred to in Articles 12 and 13 of the Regulation is provided clearly and thoroughly including with regard to the technical cookies or tools (see, in this regard, paragraph 8 below);

(iv) a command (button) through which consent can be given by accepting the storage of all cookies or the use of other tracking tools;

(v) a link to an additional dedicated area where the user can select, individually, the functionalities, the so-called third parties - whose list must be kept up-to-date whether they can be reached through ad-hoc links or via links to the websites of intermediaries representing them - and the cookies - possibly grouped into homogeneous categories - to which the user chooses to consent. If cookies are grouped into homogeneous categories and the list of the third parties changes as reflected by the links placed in this area, i.e., if additional third parties are included in the said list, it shall be for the first party (i.e., the website operator) to accurately select them and carry out the necessary supervision to ensure that the inclusion of these new entities and the resulting processing operations

continue to be in line with the grouping by homogeneous categories.

Again, compliance with privacy by default obligations requires all possible granular choices to be pre-set to refuse the storage of cookies, so that the user can only accept their storage also individually.

Where only technical cookies or similar tools are implemented, their presence may be referred to on the home page or else in the general information notice without the need to display ad-hoc banners that users will then have to remove/deactivate.

In the light of the above considerations, one can easily dispel possible misunderstandings in interpreting the user's actions by having regard to the specific configuration of the buttons and colours used by publishers - which has hitherto not been unequivocal. In that regard, it is sufficient to reiterate that - irrespective of the configuration adopted, the colours used for the buttons and, ultimately, the implementing methods chosen - the affirmative action the user is empowered to perform when first accessing a website must in any case be aimed at giving his or her consent (so-called 'opt-in') and may never consist in refusing such consent (so-called opt-out).

In this connection, the Garante would like to reiterate the importance of initiating a debate, in the most appropriate fora and among all stakeholders (academia, industry, trade associations, decision-makers, stakeholders, etc.), on the need to adopt a standardised codification of the types of controls, colours and functions to be implemented on websites in order to achieve the widest possible uniformity - for the sake of transparency, clarity and enhanced compliance. This need has been found to be unanimously felt based on the contributions from the public consultation, however it has not been catered to so far by way of proposals that could factually achieve the relevant objective.

Users will obviously be enabled to modify their choices, i.e., to give their consent after they had withheld it and to withdraw their consent – at any time, simply, easily, and in a user-friendly fashion by way of an ad-hoc area that will be accessible through a link in the website footer; that link will have to flag the underlying purpose by way of wording such as 'Change your mind on cookies' or something of that kind.

It shall be understood that whenever the banner containing the short information notice and user options is displayed again as well as whenever the user changes his or her initial choices under the terms described above, any options selected on the occasion of subsequent accesses will have to override and supersede the previous ones – i.e., the new options will apply throughout regardless of whether consent is given after it had initially been withheld or consent is withdrawn after it had initially been given.

In order to ensure that users are not influenced or affected by design arrangements such as to lead them to prefer one option over the other, it is fundamental additionally to rely on commands and characters of the same size, emphasis and colours and that all such commands and characters are equally easy to view and use.

In order to effectively enable a user to change his or her mind and therefore enforce his or her right to freely make his or her choices, the Garante is suggesting a best practice that could be identified by way of the contributions received from the public consultation. This consists in placing a graphical sign, an icon or any other technical tool on each page of the relevant domain, also close to the link to the area for selecting one's options, so as to flag – also summarily – the consent configuration applying to the given user and thus allow changing or updating such configuration at any time.

The website operator could use technical cookies (see also recital 25 of Directive 2002/58/EC), or

else other arrangements as available from technology and determined discretionally by the data controller on an accountability basis in order to record the actions and choices, including detailed ones, made by the data subject – i.e., retention of default settings; granular indication of his/her consent or withdrawal of his/her consent as previously given and reinstatement of default settings. The controller will in any case have to take the appropriate measures to keep updated records of the choices made by the individual data subject.

At all events, controllers are free to implement different mechanisms to obtain consent, for instance by having regard to the users accessing their services via authentication or access credentials. In such cases an opportunity for interrupting navigation arises naturally ever since the account creation steps have to be taken, and this would allow the controller to comply with the obligations regarding the use of cookies and other tracking tools. It should be recalled that these so-called authenticated users will have to be enabled to make informed choices – i.e., by mentioning this option also in the information notice provided to them – as to whether they should accept that they are tracked also by matching their behavior across the different devices they use.

7.2 First-party and third-party analytics cookies

Cookies can also be used, inter alia, to assess the effectiveness of an information society service provided by a publisher, to design a website or to help measure its 'traffic' - i.e. the number of visitors, possibly broken down by geographical area, time slot or other characteristics.

The Garante stated in its May 2014 decision that such identifiers, known as analytics cookies, belong with the category of technical cookies and may accordingly be used without the data subject's prior consent providing certain conditions are met. Again, the entry into force of the Regulation warrants reassessing such conditions as well as determining, in greater detail, the measures that are currently suitable for applying the exemption in question.

Firstly, it is necessary to deploy solutions to better protect the data subject through measures that are compliant with Article 25 (1) of the Regulation on privacy by design so as to 'implement data protection principles (…) in an effective manner'.

From this perspective, the Garante considers that, in the case at issue, that objective should be achieved by way of data minimization measures to significantly reduce the identification potential of analytics cookies when they are used by 'third parties'.

In other words, in order for analytics cookies to be treated on a par with technical cookies, it is essential to prevent direct identification – i.e., singling out - of the data subject through their use, which is tantamount to preventing the use of analytics cookies that can work as direct, unique identifiers on account of their features.

Accordingly, analytics cookies will have to be structured in such a way as to enable the same cookie to relate to several devices, which will create reasonable uncertainty as to the IT identity of the cookie recipient. This is usually achieved by masking out appropriate portions of the IP address in the cookie.

Taking into account the 32-bit IPv4 representation of IP addresses, which are usually represented and used as a sequence of four dot-separated decimal numbers between 0 and 255, one of the measures that can be implemented in order to benefit from the said exemption is the masking out of at least the fourth component of the address, which creates a 1/256 (approximately 0.4%) uncertainty in attributing the cookie to a specific data subject.

Similar procedures should be adopted with regard to IPv6 addresses, which have a very different structure and a significantly larger addressing space since they consist of 128-bit binary numbers.

Further, the Garante stresses the need for analytics cookies to be only used for the production of aggregated statistics and in relation to an individual website or mobile application, so as not to allow tracking an individual's navigation across different applications or websites. Accordingly, third parties providing web measurement services to the publishers shall not match the data, even if minimized in the manner described above, with any other information (such as customer records or statistics concerning visits to other websites) nor will they forward such data to other third parties since this will result into unacceptably increasing user identification risks. This is without prejudice to the production of statistics based on minimized data across several domains, websites or apps that can be traced back to the same publisher or publishing group. However, statistical analyses concerning several domains, websites or apps that can be traced back to one single controller can be considered lawful even in the absence of the aforementioned minimization measures – on condition such analyses are performed by way of the controller's own resources and do not turn into activities that go beyond statistical counting and take on ultimately the features of processing operations aimed to enable business-related decision-making.

8. New requirements applying to information notices

8.1 The information to be provided under the Regulation

Finally, the Garante would like to highlight some improvements data controllers might want to implement in order to provide information to users according to the enhanced transparency requirements set out in Articles 12 and 13 of the Regulation. This also applies to the information on any additional recipients of the personal data and the storage period of the information obtained.

It is also necessary to provide information on how natural persons can exercise all the rights provided for in the Regulation, including the right to submit an access request and to lodge a complaint with a supervisory authority.

In addition to what was laid down in the May 2014 cookie decision, and in line with the simplification rationale underlying that decision, it is the Garante's view that the information may be provided not only according to a multi-layered approach but also – by having regard to the specific context – by way of several channels and arrangements, i.e. according to a multi-channel approach. This can allow making the most of more dynamic and less traditional contact points between the data controller and the data subjects.

Examples include the increasing use of video channels, information popups, voice interactions, virtual assistants, telephone messages, chatbots, etc. .

It will then be up to the controller, who is empowered to decide on the method or the set of methods considered as most appropriate, to check that the system in place meets the requirements laid down by the Regulation in particular as for its thoroughness, clarity, effectiveness and usability.

By the same token, it will be the controller's responsibility to take all suitable measures to ensure that the information contained in the banner can be accessed without any discrimination by disabled persons who need assistive technologies or specific configurations under the terms of Law No 4 of 9 January 2004 as last amended by Law No 120 of 11 September 2020.

8.2 The need for supplementing the information to be communicated to users

The operational practice of recent years has shown that the system lacks a crucial element, especially for enforcement purposes.

Reference is made to the fact that, to date, there is no universally accepted system for semantic

coding of cookies and other tracking tools such as to allow distinguishing objectively, for example, technical cookies from analytics or profiling ones - except on the basis of the information provided by the controller in its privacy policy.

It was also found that queries and checks on the storage of cookies by a specific website may have different outcomes depending on the browser concerned.

In the light of the above, and looking forward to the expeditious achievement of overarching coding standards – which is especially important in the current connected online world, where geographical distances are becoming irrelevant in view of the increasing potential of the network – the Garante wishes to remind data controllers relying on these tools of the need to disclose, by means of an integration to the information provided, at least the coding criteria of the identifiers implemented by them. Alternatively, controllers might consider placing the said coding also within their privacy policies.

These criteria may also be communicated to the Authority upon request as a tool to support any investigative activities that will be undertaken with regard to the issues in question.

BASED ON THE ABOVE PREMISES, THE GARANTE

Under the terms of Section 154-a(1), letter a), of the Code, adopts these Guidelines in order for all providers of information society services as referred to in Article 1(1), letter (b), of Directive (EU) 2015/1535 and all the entities providing their users with publicly accessible online services through electronic communications networks or else operating websites that rely on cookies and/or other tracking tools to take account of the guidance and simplifications described in the foregoing sections with particular regard to the processing of personal data relating to the use of the functions they offer. This shall apply in particular to the following:

- Users' prior consent to the processing of the information relating to them for online tracking purposes, including information resulting from the use of cookies and other tracking tools under Section 122(4) of the Code and Article 4, item 11, and Article 7 of the Regulation, in accordance with the criteria and arrangements set out in paragraphs 6 and 7;

- Compliance with the right to withdraw one's consent under the terms of Article 7(3) of the Regulation, in accordance with the specifications made in paragraph 7.1;

- Compliance with privacy by design and privacy by default obligations as set out in Article 25 of the Regulation including by taking data minimization measures prior to their communication and use by so-called third parties, in accordance with the specifications provided in paragraph 7.2;

- The information to be provided to data subjects under Articles 12 and 13 of the Regulation with particular regard to the coding criteria applied by each controller in order to categorize cookies and other tracking tools so as to enable distinguishing technical from analytics or profiling cookies and tools, in accordance with the guidance provided in paragraph 8 of these Guidelines.

In the light of the potentially complex arrangements to be made in order to adapt the existing systems and processing operations to the principles laid down in these Guidelines, the Garante considers that the addressees hereof should bring their operations into line with the Guidelines by no later than six months from publication of the said Guidelines in the Official Journal of the Italian Republic. Attention is drawn hereby to the fact that users' consent, where already obtained and in line with the requirements under the Regulation, may be

considered to be valid on condition that the collection of such consent was recorded and is therefore duly documented also by way of IT-based evidence.

An executive summary (Annex 1) is attached to these Guidelines and shall be an integral, substantive part thereof.

A copy of these Guidelines shall be transmitted to the Ministry of Justice – Office for publication of laws and decrees in order for them to be published in the Official Journal of the Italian Republic.

Rome, 10 June 2021

THE PRESIDENT
Stanzione

THE RAPPORTEUR
Scorza

THE SECRETARY GENERAL
Mattei

(1) See recital 32 of the Regulation and Article 2 (h) of Directive 95/46/EC as compared to Article 4 (11) of the Regulation.

(2) This is the stance taken by the Court of Justice of the EU, which applied Directive 95/46 in its Wirtschaftsakademie judgment (C-210/16 of 5 June 2018) even though the case concerned processing operations falling within the material scope of the ePrivacy Directive. This also applies to the judgment in the Fashion ID case (C-40/17 of 29 July 2019).

(3) This is in line with the EDPB Opinion No 5/2019 of 12 March 2019 regarding the interplay between the two instruments as referred to in the Preamble.

(4) 'Based on recital 32, actions such as scrolling or swiping through a webpage or similar user activity will not under any circumstances satisfy the requirement of a clear and affirmative action: such actions may be difficult to distinguish from other activity or interaction by a user and therefore determining that an unambiguous consent has been obtained will also not be possible. Furthermore, in such a case, it will be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it' (see paragraph 86).