



Segreto professionale e Utilizzo di App

Avv. Lorenza Maria Villa – Avv. Antonella Rimondi

1.

Riferimenti normativi e Principi fondamentali

Art. 5 GDPR - Principi applicabili al trattamento dei dati personali

- Liceità, correttezza e trasparenza
- Limitazione delle finalità
- Minimizzazione dei dati
- Esattezza
- Limitazione della conservazione
- Integrità e riservatezza

**Privacy by Design e
Privacy By Default
(art. 25)**

**Accountability
(art. 24)**

**Regole Deontologiche relative ai trattamenti di Dati Personali
effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in
sede giudiziaria – **Provvedimento Autorità Garante n. 512 del 19.12.2019****

Il rispetto delle Regole Deontologiche costituisce:

- **La condizione di liceità del trattamento dei Dati Personali da parte degli avvocati;**

Le Regole Deontologiche:

- **Integrano le disposizioni del GDPR**
- **Specificano il principio di accountability con riferimento all'attività posta in essere dagli avvocati**

**Regole Deontologiche relative ai trattamenti di Dati Personali
effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in
sede giudiziaria – **Provvedimento Autorità Garante n. 512 del 19.12.2019****

Art. 2, comma 1

L'avvocato organizza il trattamento anche non automatizzato dei dati personali secondo le modalità che risultino più adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle libertà e della dignità degli interessati, applicando i principi di finalità, proporzionalità e minimizzazione dei dati sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste (cfr. art. 32), nonché di un'analisi della quantità e qualità delle informazioni che utilizza e dei possibili rischi.

IN PRATICA ...

ADEGUATEZZA
della sicurezza
nei trattamenti dei dati personali

finalizzata
alla tutela delle
libertà e dei diritti degli Interessati

Provvedimento Autorità Garante n. 512 del 19.12.2019

Art. 4

Specifica attenzione è prestata all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

- a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialità o che possono comportare, comunque, rischi specifici per gli interessati;
- b) **scambio di corrispondenza, specie per via telematica;**
- e) **utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tecniche e perizie, relazioni redatte da investigatori privati);**

Provvedimento Autorità Garante n. 512 del 19.12.2019

- f) Custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;
- g) Acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;**
- h) Acquisizione e conservazione di atti relativi ad affari definiti.

Art. 25 GDPR

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE

E

**PROTEZIONE DEI DATI PER IMPOSTAZIONE
PREDEFINITA**

Linee Guida EDPB n. 04/2019 – 20.11.2019

IN PRATICA ...

**La sicurezza
nei trattamenti dei dati personali
deve essere presente
dall'inizio e durante tutto il ciclo di del
trattamento fino alla cancellazione o
distruzione
dei dati personali
(che deve ugualmente avvenire con modalità sicure)**

IN PRATICA ...

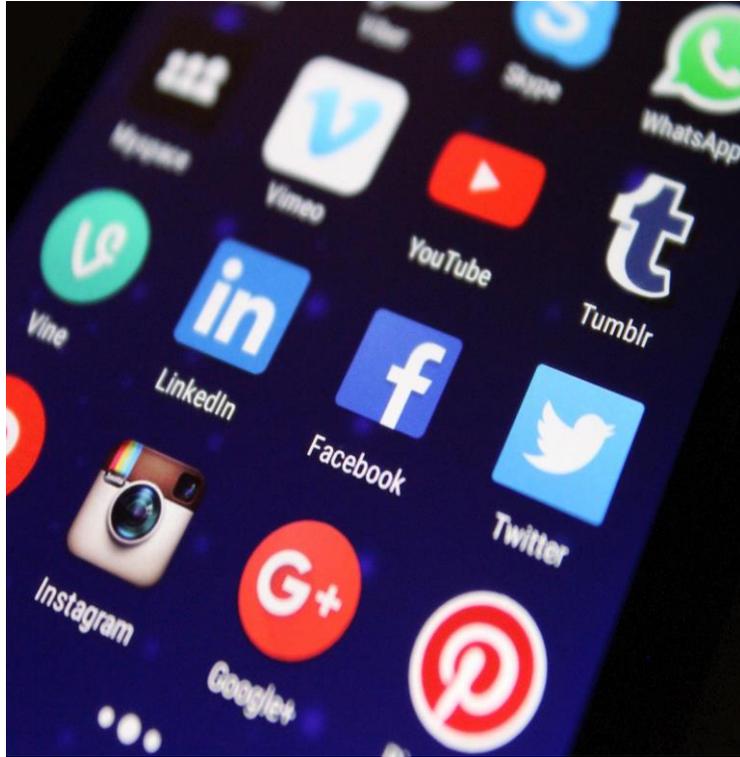
VALUTAZIONE DELL'ADEGUATEZZA DELLE CAUTELE



APPROCCIO BASATO SUL RISCHIO

tenuto conto

**della natura, dell'oggetto, del contesto, delle finalità del trattamento
della quantità e della qualità delle informazioni dello stato dell'arte e
dei costi di attuazione (Privacy by design e Privacy by default)**



Le App sono sicure ?

Dipende ...

L'uso delle App nella professione forense è condizionato dal rispetto:

- **Dei Canoni Deontologici**
- **Del GDPR e delle Regole del Garante**
- **Segreto professionale**
- **Riservatezza, Integrità e Disponibilità del dato**
- **Art. 5, 24 e 25 GDPR e Regole del Garante**
- **Misure di sicurezza tecniche (cybersecurity)**
- **Misure di sicurezza organizzative (comportamentali)**

2.

App e Professione Forense

Apps By Design



... scegliere una App

STEP I : Comparazione delle app alla luce dei principi del GDPR

	SIGNAL	THREEMA	TELEGRAM	WHATSAPP FB		SIGNAL	THREEMA	TELEGRAM	WHATSAPP FB
PROVENTI / FINANZIAMENTI	Donazioni	Una tantum all'iscrizione	Donazioni	Publicità + FB	CASI DI DISCLOSURE DI DATI ALLE AGENZIE DI INTELLIGENCE	NO	NO	NO	SI
CRITTOGRAFIA END-TO-END	SI	SI	SI	SI	DATI PERSONALI RACCOLTI	N. TEL	EMAIL N. TEL ID UTENTE	NOME, N. TEL, DATI DEI CONTATTI, ID UTENTE	
CRITTOGRAFIA ATTIVATA BY DEFAULT	SI	SI	SOLO NELLE CHAT SEGRETE	SI	CRITTOGRAFIA DEI DATI DEI CONTATTI	SI	SI	NO	NO
IL PROVIDER LEGGE IL CONTENUTO DEI MESSAGGI?	NO	NO	NELLE CHAT ORDINARIE	NO	CONDIVISIONE INFORMAZIONI CON TERZI	NO	NO	NO	
BACK-UP MESSAGGI	SU DEVICE	SU DEVICE	SU CLOUD DI PROPRIETA'	GOOGLE CLOUD SENZA CRITTOGRAFIA					
GIURISDIZIONE COMPAGNIA	USA	SVIZZERA	DUBAI	USA					
GIURISIDIZIONE DELLE INFRASTRUTTURE (DATA CENTER)	USA	SVIZZERA	OLANDA (residenti UE – UK)	USA					

STEP 1: Comparazione delle app alla luce dei principi del GDPR

WhatsApp 'Data Linked To You'	Facebook Messenger 'Data Linked To You'
<p>Analytics</p> <ul style="list-style-type: none"> Purchases Purchase History Location Coarse Location Contact Info Phone Number User Content Other User Content Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Diagnostics Crash Data Performance Data Other Diagnostic Data <p>App Functionality</p> <ul style="list-style-type: none"> Purchases Purchase History Financial Info Payment Info Location Coarse Location Contact Info Email Address Phone Number Contacts Contacts User Content Customer Support Other User Content Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Diagnostics Crash Data Performance Data Other Diagnostic Data 	<p>Third-Party Advertising</p> <ul style="list-style-type: none"> Purchases Purchase History Financial Info Other Financial Info Location Precise Location Coarse Location Contact Info Physical Address Email Address Name Phone Number Other User Contact Info Contacts Contacts User Content Photos or Videos Gameplay Content Other User Content Search History Search History Browsing History Browsing History Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Other Usage Data Diagnostics Crash Data Performance Data Other Diagnostic Data Other Data Other Data Types <p>Analytics</p> <ul style="list-style-type: none"> Health & Fitness Health Fitness Purchases Purchase History Financial Info Payment Info Other Financial Info Location Precise Location Coarse Location Contact Info Physical Address Email Address Name Phone Number Other User Contact Info Contacts Contacts User Content Photos or Videos Gameplay Content Other User Content Search History Search History Browsing History Browsing History Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Other Usage Data Sensitive Info Sensitive Info Diagnostics Crash Data Performance Data Other Diagnostic Data Other Data Other Data Types <p>Product Personalisation</p> <ul style="list-style-type: none"> Purchases Purchase History Financial Info Other Financial Info Location Precise Location Coarse Location Contact Info Physical Address Email Address Name Phone Number Other User Contact Info Contacts Contacts User Content Photos or Videos Gameplay Content Other User Content Search History Search History Browsing History Browsing History Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Other Usage Data Sensitive Info Sensitive Info Diagnostics Crash Data Performance Data Other Diagnostic Data Other Data Other Data Types <p>App Functionality</p> <ul style="list-style-type: none"> Health & Fitness Health Fitness Purchases Purchase History Financial Info Payment Info Credit Info Other Financial Info Location Precise Location Coarse Location Contact Info Physical Address Email Address Name Phone Number Other User Contact Info Contacts Contacts User Content Photos or Videos Gameplay Content Customer Support Other User Content Search History Search History Browsing History Browsing History Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Other Usage Data Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Other Usage Data Sensitive Info Sensitive Info Diagnostics Crash Data Performance Data Other Diagnostic Data Other Data Other Data Types <p>Other Purposes</p> <ul style="list-style-type: none"> Purchases Purchase History Financial Info Other Financial Info Location Precise Location Coarse Location Contact Info Physical Address Email Address Name Phone Number Other User Contact Info Contacts Contacts User Content Photos or Videos Gameplay Content Customer Support Other User Content Search History Search History Browsing History Browsing History Identifiers User ID Device ID Usage Data Product Interaction Advertising Data Other Usage Data Diagnostics Crash Data Performance Data Other Diagnostic Data Other Data Other Data Types

STEP 2: scelta della App e compliance al GDPR

- FINALITA' → MINIMIZZAZIONE
- DATI / INFORMAZIONI PERSONALI TRATTATE → MINIMIZZAZIONE
- UTILIZZATORE DELLO SMARTPHONE E DELL'APP → AUTORIZZAZIONI ?
- BASE GIURIDICA DEL TRATTAMENTO → CONSENSO

INTERESSE LEGITTIMO

- trattamento necessario rispetto alle finalità perseguite?
- sono effettivamente tutelati i diritti e le libertà fondamentali degli interessati?
- l'Interesse legittimo prevale sui diritti e sulle libertà degli interessati? Legittima aspettativa dell'interessato rispetto al trattamento
- tutela del diritto di opposizione → informativa

STEP 2: scelta della App e compliance al GDPR

- **TRASFERIMENTO DI DATI AL DI FUORI DELL'UE**
 - SUSSISTENZA DELLE GARANZIE PREVISTE DAL GDPR / DEROGHE / CONSENSO
 - INFORMATIVA
- **TEMPO DI CONSERVAZIONE**
- **MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE**
- **ANALISI DEL RISCHIO**
- **IMPLEMENTAZIONE DI ULTERIORI MISURE DI SICUREZZA**
- **DPIA?**

STEP 2: scelta della App e compliance al GDPR

➤ MISURE DI SICUREZZA TECNICHE

GENERICHE (SMARTPHONE)

- PIN o A2F
- Antivirus
- VPN
- Blocco temporizzato schermo
- Crittografia device

SPECIFICHE (APP - SIGNAL)

- Inibizione dei Pop-Up
- Tastiera in incognito
- Blocco schermo con temporizzazione
- PIN
- Verifica periodica del PIN
- Registrazione su nuovo device con PIN

STEP 2: scelta della App e compliance al GDPR

➤ MISURE DI SICUREZZA ORGANIZZATIVE

- Navigazione in VPN quando connessi a WI-FI (in particolare WI-FI pubblico)
- Digitazione PIN lontano da possibili osservatori
- Attivazione di sistemi antifurto
- Istruzioni a utilizzatori diversi dal titolare dell'App
- Disinstallazione dell'App nel caso di necessità di riparazioni / dismissione / cessione del device
- Cancellazione periodica delle chat con eventuali back-up su unità esterna

STEP 2: scelta della App e compliance al GDPR

➤ MISURE DI SICUREZZA ORGANIZZATIVE

AGGIORNAMENTI IN MODALITA' AUTOMATICA

CONTROLLO PERIODICO DELLE IMPOSTAZIONI DELL'APP



WhatsApp & THE PRIVACY ...

Gennaio 2021

WhatsApp: Garante privacy, informativa agli utenti poco chiara - L'Autorità intenzionata ad intervenire anche in via d'urgenza

Il messaggio con il quale WhatsApp ha avvertito i propri utenti degli aggiornamenti che verranno apportati, dall'8 febbraio, nei termini di servizio - in particolare riguardo alla condivisione dei dati con altre società del gruppo - e la stessa informativa sul trattamento che verrà fatto dei loro dati personali, sono poco chiari e intelligibili e devono essere valutati attentamente alla luce della disciplina in materia di privacy.

Per questo motivo il Garante per la protezione dei dati personali ha portato la questione all'attenzione dell'[Edpb](#), il Board che riunisce le Autorità privacy europee.

Il Garante ritiene che dai termini di servizio e dalla nuova informativa non sia possibile, per gli utenti, evincere quali siano le modifiche introdotte, né comprendere chiaramente quali trattamenti di dati saranno in concreto effettuati dal servizio di messaggistica dopo l'8 febbraio.

Tale informativa non appare pertanto idonea a consentire agli utenti di Whatsapp la manifestazione di una volontà libera e consapevole.

Il Garante si riserva comunque di intervenire, in via d'urgenza, per tutelare gli utenti italiani e far rispettare la disciplina in materia di protezione dei dati personali.

Roma, 14 gennaio 2021

Fonte: GPDP - <https://www.garanteprivacy.it/home/docweb/-/docwebdisplay/docweb/9519943>

WhatsApp & THE PRIVACY ...

“Non ci sono modifiche alle modalità di condivisione dei dati di WhatsApp nella Regione europea, incluso il Regno Unito, derivanti dall’aggiornamento dei Termini di servizio e dall’Informativa sulla privacy. Non condividiamo i dati degli utenti dell’area europea con Facebook allo scopo di consentire a Facebook di utilizzare tali dati per migliorare i propri prodotti o le proprie pubblicità”. FONTE: ANSA



WhatsApp & THE PRIVACY ...

“Oggi Facebook non usa le informazioni del tuo account WhatsApp per migliorare le tue esperienze con i prodotti di Facebook. Qualora in futuro decidessimo di condividere tali dati con le aziende di Facebook per questo scopo, lo faremo solo dopo aver raggiunto un accordo con la commissione per la protezione dei dati irlandese”.

Niamh Sweeney, Director of Policy for WhatsApp, EMEA on Twitter



WhatsApp & THE PRIVACY ...

15 Gennaio 2021

“modifiche che riguardano nuove opzioni facoltative a disposizione degli utenti che desiderano comunicare con le aziende su WhatsApp e offre maggiore trasparenza sulle nostre modalità di raccolta e utilizzo dei dati”.
“L’8 febbraio, nessun account verrà sospeso o eliminato. Continueremo a impegnarci per fare chiarezza sulle informazioni errate riguardanti la sicurezza e la privacy su WhatsApp. In modo graduale, e secondo le tempistiche di ciascuno, inviteremo i nostri utenti a rivedere **l’informativa prima del 15 maggio, quando saranno disponibili le nuove opzioni business**”.



Posticipo al 15 maggio dei termini di accettazione della nuova policy

WhatsApp & THE PRIVACY ...



15 maggio 2021

Stiamo aggiornando i nostri termini e l'informativa sulla privacy

Prima che tu li riveda, ci sono alcune cose da sapere.



Non possiamo leggere né ascoltare le tue conversazioni personali, perché sono protette dalla crittografia end-to-end. E lo saranno sempre.



Stiamo rendendo più facili le conversazioni con le aziende per consentire di fare domande e ricevere risposte in modo rapido. Chattare con le aziende è facoltativo.



È nostra responsabilità spiegare che cosa stiamo modificando, per questo abbiamo messo a disposizione maggiori informazioni in [questa pagina](#).

• •

CONTINUA

Aggiornamento dei Termini e dell'Informativa sulla privacy di WhatsApp



Non stiamo apportando modifiche alla privacy delle tue conversazioni personali.

Questo [aggiornamento](#) dei nostri Termini e della nostra Informativa sulla privacy fornisce maggiori informazioni, anche in merito a come puoi comunicare con le aziende, se lo desideri. Questo include:



Come le aziende possono gestire le chat grazie agli strumenti di Facebook. Le chat con queste aziende sono facoltative e sono contrassegnate chiaramente nell'app.



Maggiori informazioni su come funziona WhatsApp, incluse le modalità di trattamento dei dati e come garantiamo la sicurezza del tuo account.

I [termini](#) entreranno in vigore il 15 maggio 2021. Ti invitiamo ad accettarli per continuare a usare WhatsApp dopo questa data. Per maggiori informazioni sul tuo account, ti invitiamo a leggere [questa pagina](#). Per saperne di più su come elaboriamo i tuoi dati, consulta la nostra [informativa sulla privacy](#) aggiornata.

• •

ACCETTA

WhatsApp & THE PRIVACY ...



15 maggio 2021

In caso di non adesione ai nuovi termini, l'utente subirà progressivamente le seguenti limitazioni:

- Cessazione dell'accesso all'elenco delle chat con possibilità di rispondere solo ai messaggi e alle chiamate in arrivo
- Successiva disattivazione delle chiamate in arrivo e delle notifiche
- Inibizione della possibilità di esportare la cronologia chat su Android o iPhone e di scaricare il rapporto dell'account.
- Cancellazione dell'account

WhatsApp & THE PRIVACY ...

Policy
15 maggio 2021



«WhatsApp viene utilizzato da quasi 60 milioni di persone in Germania ed è di gran lunga l'applicazione social più usata, anche più di Facebook. Diventa quindi ancora più importante garantire che il gran numero di utenti, che rende il servizio attraente per molte persone, non porti ad uno sfruttamento non autorizzato dei dati.»

**Autorità Garante di
Amburgo**

**Procedimento d'urgenza contro
Facebook Ireland**

**Richiesta di ordine volto ad
impedire la raccolta e
l'elaborazione dei dati personali
degli utenti di WhatsApp.**

WhatsApp & THE PRIVACY ...



- (Il Sole 24 Ore Radiocor Plus) - Milano, 14 mag - Facebook ha visto respingere dalla giustizia irlandese la sua richiesta di bloccare una inchiesta delle autorità di controllo irlandesi, **che potrebbe impedire il trasferimento di dati personali dall'Ue agli Stati Uniti**. L'Alta corte irlandese, su richiesta di Facebook, aveva accettato lo scorso settembre di sospendere temporaneamente l'inchiesta della Commissione per la protezione dei dati ma oggi ha ribaltato quella decisione e ha respinto la richiesta di bloccare l'inchiesta.

WhatsApp & THE PRIVACY ...



Sentenza Facebook in Irlanda.

Scorza: "Trema l'ecosistema digitale, ecco l'unica soluzione"
Intervento di Guido Scorza, componente del Garante per la protezione dei dati personali .(*Agenda Digitale, 18 maggio 2021*)

L'ecosistema digitale trema come durante un terremoto di magnitudine senza precedenti, dopo la sentenza dello scorso 12 maggio dell'Alta Corte irlandese.

L'Alta Corte, respingendo il ricorso di Facebook, ha stabilito che non sussistono ostacoli a che il Garante irlandese per la protezione dei dati personale prosegua e concluda il procedimento avviato nei confronti del social network di Mark Zuckerberg in relazione al trasferimento negli Stati Uniti d'America dei dati personali dei cittadini europei.



WhatsApp & THE PRIVACY ...

EUROPEAN PARLIAMENT CALLS ON COMMISSION TO OPEN INFRINGEMENT PROCEEDING AGAINST IRELAND



The European Parliament has adopted a resolution calling on the European Commission to start infringement procedures against Ireland, over the lack of GDPR enforcement. Today the votes became public: The resolution was adopted by a vast majority of 541 votes, with only one vote by an independent Member against the resolution 151 members abstained from the vote.

The resolution took special issues with the Irish Data Protection Commission: The European Parliament "*expresses deep concern that several complaints against breaches of the GDPR filed on 25 May 2018, the day the GDPR became applicable, and other complaints from privacy organisations and consumer groups, have not yet been decided by the DPC, which is the lead authority for these cases.*"

It further highlighted that it "*is concerned that the DPC interprets 'without delay' in Article 60(3) of the GDPR – contrary to the legislators' intention – as longer than a matter of months.*"

The Parliamentarians also called on other Data Protection Authorities in the EU to "*take proactive steps under Article 61 and 66 of the GDPR to force the DPC to comply with its obligations under the GDPR*".

The Austrian MEP Bettina Vollath used the debate on the resolution to read out a statement by Max Schrems, calling on improved enforcement of the GDPR.

<https://noyb.eu/en/european-parliament-calls-commission-open-infringement-proceedings-against-ireland>



Think Before You click
Of...
Before you «App»



Avv. Lorenza Maria Villa – Avv. Antonella Rimondi