Presto, molto presto, entrerà in vigore. Il “famigerato” GDPR, perché non si contano gli annunci e gli articoli, dai toni talvolta allarmistici, sugli organi di informazione e sulle testate giornalistiche dell'ICT.

GDP*Ready (or not?)*

Essere conforme è la regola, essere *Pronti* non deve essere l’eccezione.
GDPR Compliance: facilitare le Aziende nella **gestione rapida, regolamentata e semplice** delle **interazioni con i clienti**.

“Accountability”

E’ il principio-pilastro del GDPR, ma è poco traducibile dall’inglese. Diciamo **responsabilità + competenza + affidabilità + trasparenza**.

Sono le quattro fondamenta su cui armonizzare diverse legislazioni nazionali, più o meno permissive, per incoraggiare un **dialogo rispettoso del cittadino/cliente**.

L’azienda che tratta dati personali deve essere in grado di **rendere conto** a terzi della gestione di questi dati: dal consenso informato in poi.

Non tutte le responsabilità vengono per nuocere, possono anzi trasformarsi in opportunità. Vediamone alcune:

1. **Riponderare la compravendita di liste di contatti**
2. **Rispettare il diritto all’oblio**
3. **La trasparenza paga!**

Recap:

#1

Designazione del DPO, Data Protection Officer.

#2

Costituzione del Registro delle attività di trattamento.

#3

Individuazione di procedure organizzative e di notifica delle violazioni di dati personali.

That’s it?

[…] Di fatto, **si reintroduce l’obbligo di acquisizione del consenso per larga parte delle ipotesi di trattamento di dati a fini di marketing**, depotenziando così la portata della base giuridica del legittimo interesse del titolare e le chiare indicazioni del considerando 47 del regolamento.

Ciò detto, osserviamo che il comma 1 dell’art. 88 introduce l’obbligo di consenso del contraente o dell’utente per l’invio di comunicazioni promozionali con l’uso di **sistemi automatizzati di chiamata**.

Passi il fatto che la “molestia” di questa forma di marketing possa aver indotto il nostro legislatore ad una soluzione che reintroduca la necessità del consenso, ma più incomprensibile è la previsione del comma 2 dell’articolo, che estende la disposizione del comma 1 anche alle **comunicazioni elettroniche a fini di marketing, quali e-mail e sms**: anche per tali comunicazioni, quindi, serve il consenso.

L’art. 7 dell’art. 88, infine, reintroduce il c.d. soft spam già previsto dall’art. 130 del D.Lgs. 196/03; in verità, peraltro, mentre il Garante aveva esteso l’ambito di applicazione del soft spam anche alla posta cartacea, il decreto legislativo (evidentemente “frettolosamente” confezionato) non ne tiene conto, e si limita a contemplare nel comma in esame solo “le coordinate di posta elettronica”.

Se così è, di fatto, **poco spazio resta per il marketing fondato sul legittimo interesse**. Potrebbe essere il caso dei biglietti da visita raccolti presso l’interessato, o qualche ipotesi simile.

Come se non bastasse, infine, l’art. 79, comma 2, lettera f definisce “contraente” anche la persona giuridica; e poiché l’art. 88 si riferisce anche al consenso del “contraente”, ecco che pure **i dati delle persone giuridiche tornano ad essere oggetto di tutela in ambito privacy** (in piena contraddizione con un principio cardine del Gdpr, e cioè che lo stesso tutela solo i dati delle persone fisiche). […]

Credits: CorCom / Studio Legale Giacopuzzi, 30.03.18

That’s it?

Diversamente da quanto pubblicato su Agendadigitale.eu, il Garante Privacy fa sapere di non “essersi pronunciato su un ipotetico periodo di grazia” durante il quale non sanzionerebbe le aziende che, a seguito di ispezioni, fossero inadempienti rispetto ai nuovi obblighi normativi introdotti dal Regolamento europeo.

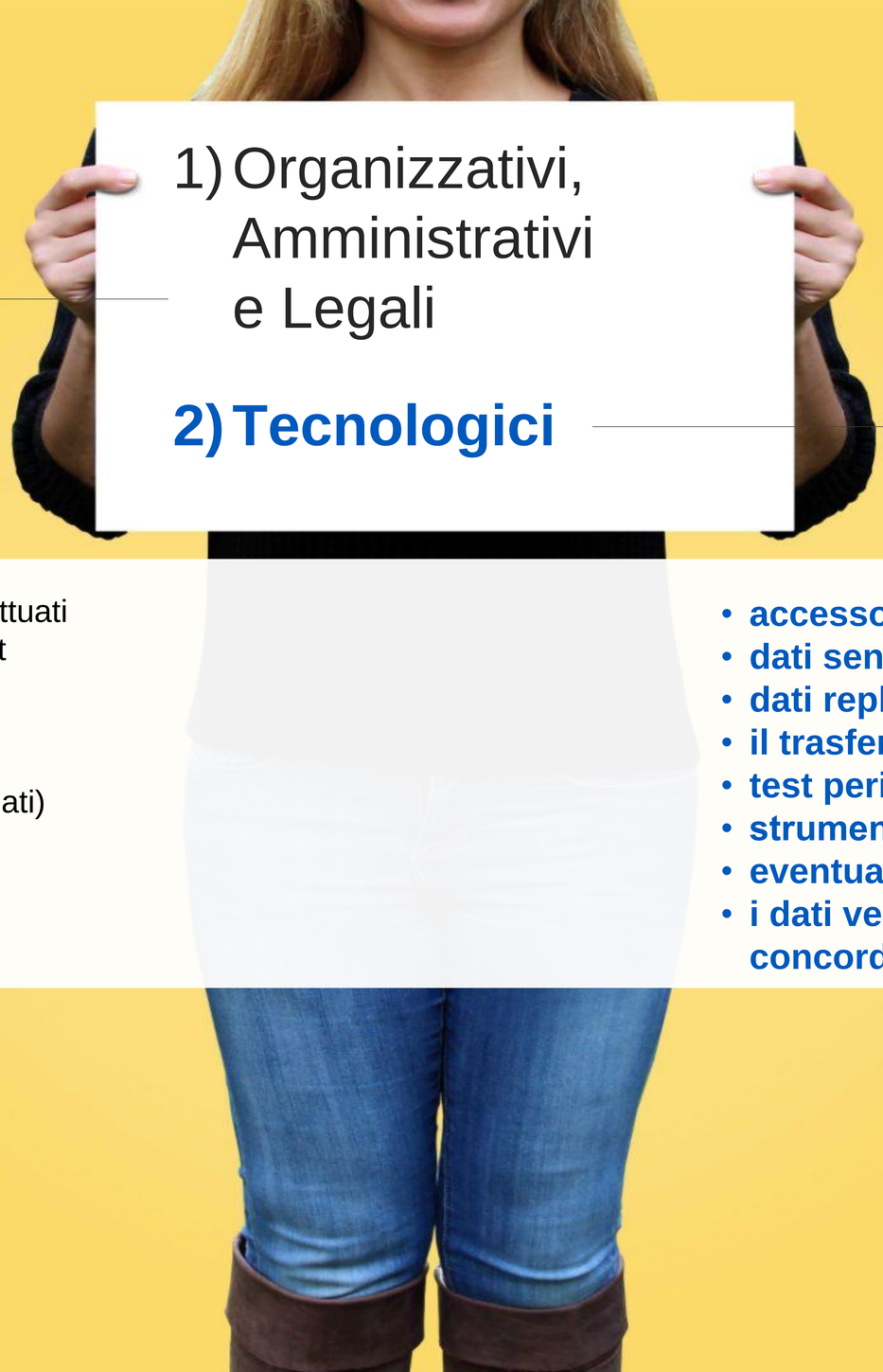
Per cui risulta falsa la notizia secondo cui l’Autorità per la protezione dei personali “ha congelato di 6 mesi le sanzioni alle aziende dopo l’entrata in vigore del Gdpr”. A Key4biz l’Authority ha dichiarato “**Non ci siamo pronunciati su un ipotetico periodo di grazia** e il provvedimento citato non ha nessun nesso con il tema delle sanzioni”.

[…] Ad essere differite sono le specifiche indicazioni che il legislatore aveva previsto venissero inserite nel provvedimento, ma non certo le **disposizioni** del Regolamento, che **si applicheranno inderogabilmente a partire dal 25 maggio**.

A quanto ammontano le sanzioni previste dal Gdpr?
«Chi non rispetta il regolamento rischia sanzioni fino a 20 milioni di euro o al 4% del fatturato internazionale annuo lordo.»

Credits: Key4Biz / Garante Privacy, 19.04.18

Interventi:



- **analisi dei rischi** relativi ai trattamenti effettuati
- stesura di un **DPIA** -Data Protection Impact Assessment- per ogni processo gestito dall'azienda
- aggiornamento della **contrattualistica** (es. nomina Responsabile del trattamento dei dati)


YourVoice

Nomina a Responsabile del Trattamento Dati

Your Voice S.p.A.

- **accesso ai dati via credenziali nominali tracciate**
- **dati sensibili criptati a livello di applicazione**
- **dati replicati su più data center**
- **il trasferimento dati avviene via canali cifrati**
- **test periodici di vulnerabilità**
- **strumenti per l’export e la cancellazione dei dati**
- **eventuali storici di dati sono anonimizzati**
- **i dati vengono mantenuti solo per il tempo concordato**

In sintesi, cosa prevede il GDPR

La nuova normativa si applica ai **cittadini UE**, ovunque risiedano nel mondo, alle **aziende europee** e a qualsiasi azienda **anche extra-UE** che voglia o debba gestire dati personali di cittadini UE e/o il monitoraggio del loro comportamento all'interno dell'UE.

Per contattare una persona, e raccoglierne e gestirne i dati personali, a un'azienda occorre un **motivo valido**.

Occorre poter **dimostrare il consenso**, fornito da una persona, al trattamento dei propri dati.

La persona deve poter, in qualsiasi momento, **accedere** ai propri dati, modificarli, **verificare** lo stato del suo consenso (oggetto e finalità per cui era stato prestato) ed eventualmente revocarlo.

La persona ha il diritto di poter richiedere la completa e definitiva **eliminazione** dei propri dati personali memorizzati presso l'azienda.

C’è dato,
e dato,
e dato.

dati personali **ANAGRAFICI**
Es. nome e cognome, carta di identità, passaporto, residenza…

dati personali **ONLINE**
Es. indirizzi IP, cookies, tag RFID, GPS…

dati personali **PARTICOLARI / SENSIBILI**
Es. cartella clinica, orientamento religioso, orientamento sessuale, orientamento politico, etnia, impronte digitali, genoma…

3 x Privacy

01 Privacy by design

Significa che **ogni nuovo servizio o processo aziendale** che utilizza i dati personali deve prendere in considerazione la protezione di quei dati. Le aziende devono essere in grado di dimostrare che hanno **adottato** un adeguato grado di sicurezza e che **monitorano** la Compliance. La protezione dei dati deve essere un aspetto determinante lungo l'intero ciclo di sviluppo di un nuovo sistema.

02 Privacy by default

Significa che quando un cliente acquista un nuovo prodotto o servizio vengono applicate automaticamente le **impostazioni di privacy più rigorose**. In altri termini, non dovrebbero essere necessarie modifiche manuali alle impostazioni sulla privacy da parte dell'utente. I titolari o i responsabili del trattamento potranno archiviare dati solo per il **tempo** strettamente necessario a fornire un prodotto o servizio.

03 Pseudonimizzazione

E' una tecnica di protezione della privacy in cui i dati personali trattati **non possono essere attribuiti a una persona specifica**. Le informazioni vengono rese non attribuibili a una persona senza l'utilizzo di informazioni aggiuntive, che devono essere conservate **separatamente** e soggette a misure tecniche e controlli organizzativi. Il loro utilizzo è incoraggiato dal GDPR e identificato come misura di sicurezza.

(fonte: F-Secure, www.f-secure.com)

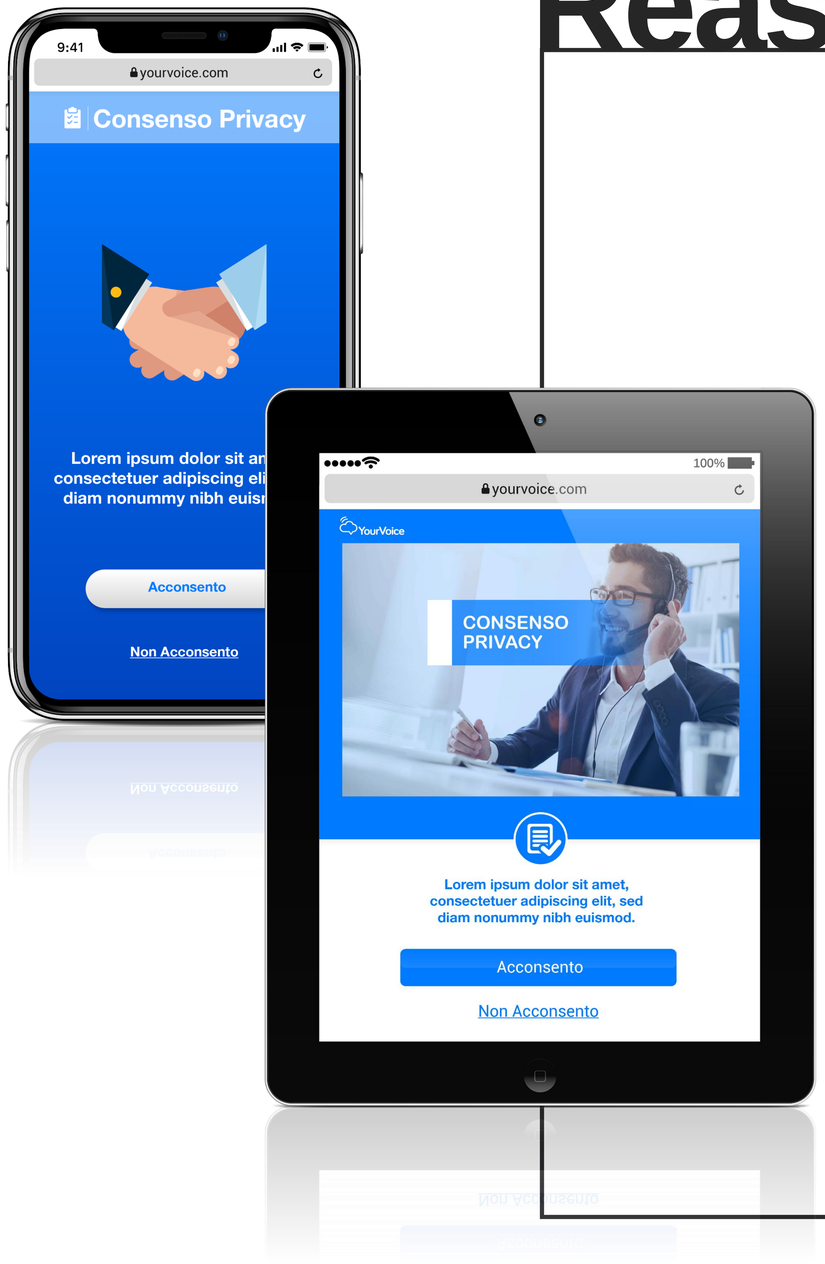
Attività Minima Urgente

Quali sono le attività minime necessarie che le aziende dovrebbero assolutamente portare a termine entro il 25 maggio per non incorrere in sanzioni?

«Un'azienda dovrà dimostrare di avere avuto un approccio responsabile e proattivo rispetto al Gdpr.
Più in concreto, dovrà aver censito i trattamenti di dati personali che vengono condotti presso la propria organizzazione. Dovrà, quindi, aver valutato se tali trattamenti vengono svolti nel rispetto delle nuove disposizioni e, quindi, aver effettuato gli interventi ritenuti necessari.
Ad esempio, ove un trattamento sia basato sul consenso degli interessati, **il titolare dovrà preoccuparsi di verificare che i consensi acquisiti in precedenza siano validi anche ai sensi della nuova normativa**.»

(fonti:
Avv. Massimiliano Pappalardo,
Certified Information Privacy Professional Europe,
Studio Legale D&P;
ComputerWorldItalia)

Reasons Why



RISPARMI SUI COSTI

Impiegare comunicazioni massive, con sensibili risparmi sui costi: fino al 50% vs telemarketing, e liberando le risorse pregiate sulle attività core business.

EVITI LE SANZIONI

Non per fare del terrorismo psicologico gratuito, ma l'adeguamento al GDPR è un obbligo di legge e le sanzioni potranno ammontare fino a 10 o 20 milioni di €, a seconda dei casi, o pari rispettivamente al 2% o al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

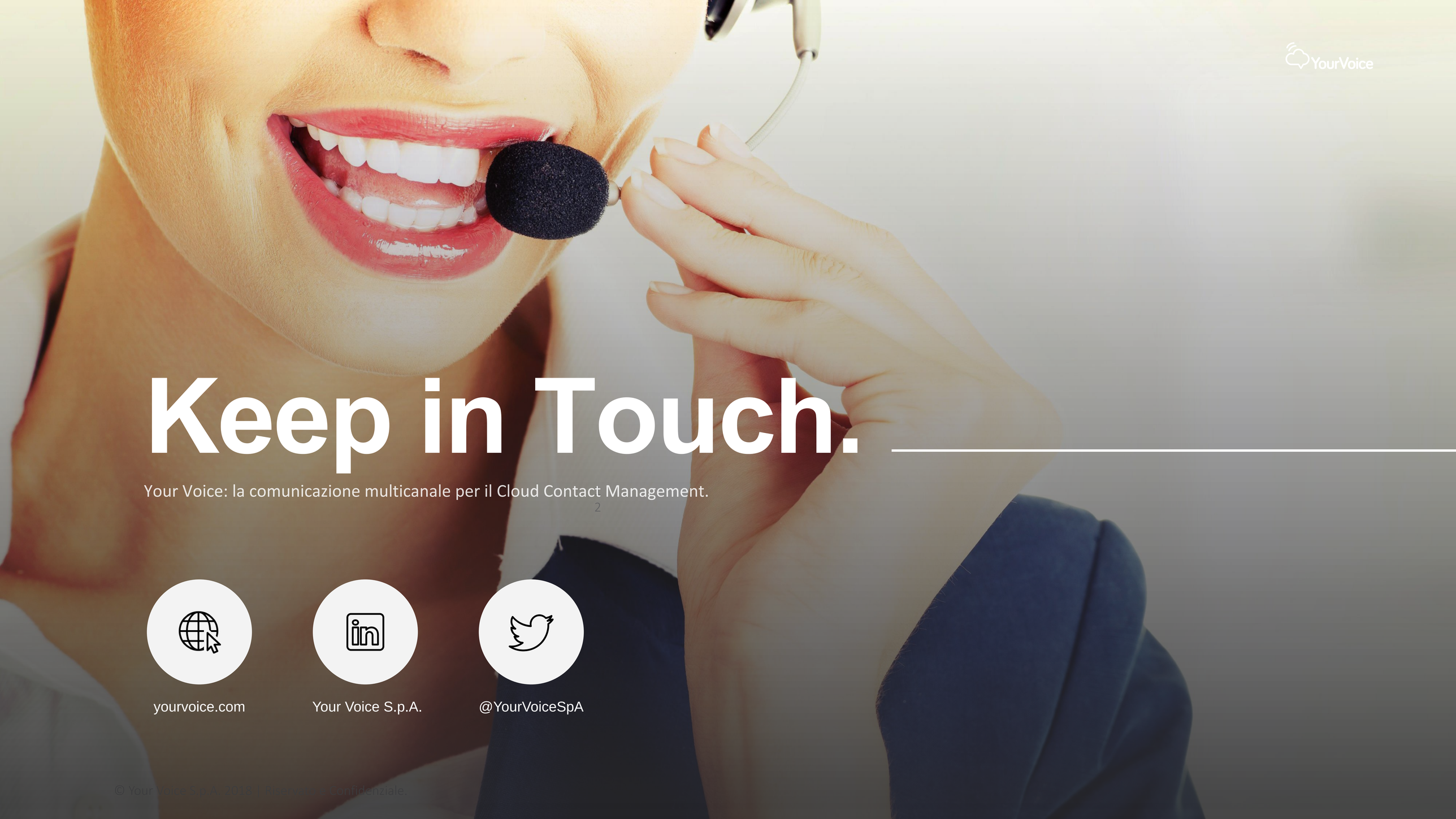
CONSENSO RAPIDO

Ridurre in modo drastico il tempo medio di gestione di un contatto, offrendo feedback veloci e precisi dalla base clienti.

CONTROLLO E SICUREZZA

In caso di campagne Visual CX, il link inviato al cliente tramite SMS è:

- univoco per ogni sessione/cliente
- configurabile in termini di timeout
- integrabile con funzionalità OTP
- tracciabile per generare statistiche su views, tap…



Keep in Touch.

Your Voice: la comunicazione multicanale per il Cloud Contact Management.

yourvoice.com

Your Voice S.p.A.

@YourVoiceSpA