PRESENTAZIONE
GDPR
E
FATTURAZIONE ELETTRONICA

ITALSOLUZIONI s.r.l. - Via Giuseppe Ungaretti, 7 – 14053 Canelli (AT)- Tel 0141-831014
Mail: info@italsoluzioni.com sito: www.italsoluzioni.com

ITALSOLUZIONI

General
Data Protection
Regulation

Il **GDPR**, acronimo di General Data Protection Regulation, è il nuovo regolamento europeo con cui si definiscono i diritti dei cittadini europei circa il **trattamento dei propri dati personali** da parte delle aziende.

Il regolamento è già in vigore dal 2016 ed è diventato pienamente operativo **a decorrere dal 25 maggio 2018.**

Lo strumento del Regolamento: Efficacia diretta

Questo Regolamento ha effetti legali diretti in tutti gli Stati Membri.

A differenza della direttiva, **non deve essere recepito a livello nazionale.**

Nell'articolo 4 del GDPR vengono fornite le definizioni di «**Dato personale**» e di «**Trattamento di un dato**».
Vediamo le relative definizioni.

COSA SI INTENDE PER DATO PERSONALE

Ai fini del regolamento per "**dato personale**" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato");

Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come ad esempio:

- nome e cognome
- indirizzo di casa
- indirizzo email
- data di nascita
- luogo di nascita
- numero di telefono
- account name o nickname
- numero di targa del veicolo
- Eccetera ….

Cos’è il trattamento di un dato?

Qualsiasi attività di **gestione del dato** come:

- ✓ la raccolta
- ✓ la conservazione
- ✓ la modifica
- ✓ la consultazione
- ✓ la comunicazione
- ✓ la cancellazione

Su qualsiasi supporto:

- ✓ informatico
- ✓ cartaceo o analogico,

sia attraverso operatori sia con processi automatizzati

I Principi su cui si basa il GDPR

Gli elementi di liceità del trattamento (40-44)

Il trattamento è lecito solo quando si fonda su una base di legittimità come il

Consenso: l'interessato ha dato il consenso al trattamento dei propri dati personali per uno o più scopi specifici;

Esecuzione contrattuale: l'elaborazione è necessaria per l'esecuzione di un contratto di cui l'interessato è parte;

Obbligo legale: l'elaborazione è necessaria per adempiere a un obbligo legale a cui è soggetto il responsabile del trattamento;

Interesse vitale delle persone: il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica;

Interesse pubblico: il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri conferiti al responsabile del trattamento;

Interesse legittimo: il trattamento è necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da una terza parte

Il Principio di Correttezza

La correttezza del trattamento è essenzialmente legata all'idea che gli interessati devono essere consapevoli del fatto che i loro dati personali saranno trattati, **per consentire loro di prendere una decisione informata**.

Il Principio di Trasparenza

Il principio di trasparenza impone che le informazioni e **le comunicazioni** relative al trattamento di tali dati personali siano **facilmente accessibili e comprensibili** e che sia utilizzato un linguaggio semplice e chiaro.

Il Principio di Limitazione delle Finalità

I Titolari devono innanzitutto identificare **le particolari finalità** per le quali i dati personali saranno trattati **(by design). Tali scopi diverranno i limiti** entro i quali i dati personali devono essere raccolti e utilizzati dai responsabili del trattamento dei dati.

Il principio di minimizzazione dei dati

Il principio della « minimizzazione dei dati" indica che un Titolare del trattamento dei dati dovrebbe **limitare la raccolta di informazioni personali a ciò che è direttamente rilevante e necessario per raggiungere uno scopo specifico.**
Dovrebbero inoltre conservare i dati solo per il tempo necessario a raggiungere lo scopo.

Il Principio di Esattezza

I dati raccolti **dovranno essere esatti** e, se necessario, aggiornati. Di conseguenza le Aziende dovranno adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente eventuali dati inesatti rispetto alle finalità per le quali sono trattati.

Il Principio di Limitazione della conservazione

Il GDPR non stabilisce alcun periodo minimo o massimo per la conservazione dei dati personali ma **non devono essere conservati per un periodo superiore a quello necessario** per tale scopo o per tali finalità.

Il Principio di integrità e riservatezza

I dati dovranno essere sempre trattati in maniera da **garantire una sicurezza adeguata**, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

La tutela della riservatezza «by design» e «by default»

IL PRINCIPIO DI «PRIVACY BY DESIGN» SEGNA UN NETTO CAMBIAMENTO DI APPROCCIO ALLA PROTEZIONE DEI DATI PERSONALI DEGLI INTERESSATI

Nel D.Lgs 196/2003
PREVISIONE DI STANDARD MINIMI PER IL TRATTAMENTO DEI DATI

Con il Regolamento Europeo 2016/679
APPROCCIO PROATTIVO

Art. 4 -Definizioni

D.Lgs. 196/2003

"misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31

R.E. 2016/679

Il titolare del trattamento è competente per il rispetto del paragrafo1 e in grado di comprovarlo («responsabilizzazione»).
Principio di Accountability

Protezione dei dati fin dalla progettazione **(by design)** e protezione per impostazione predefinita**(by default)**
…il titolare del trattamento mette in atto misure tecniche e organizzative adeguate…
…per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento… **(Principio di minimizzazione)**

«Pseudonimizzazione e cifratura dei dati»

Il trattamento dei dati personali è posto in essere in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile» (art. 4.5), GDPR

Le figure coinvolte

Interessato	▪ la persona fisica di cui si raccolgono e trattano dati personali di varia natura
Il titolare del trattamento	▪ il legale rappresentante dell'organizzazione che raccoglie e tratta i dati personali degli interessati
Il responsabile del trattamento	▪ la persona incaricata dal titolare per il trattamento
L'incaricato al trattamento dei dati	▪ la persona che nelle sue mansioni utilizza i dati personali
Il responsabile protezione dati (DPO)	▪ una persona esperta di legislazione e pratiche relative alla protezione dei dati deve assistere colui che li controlla o li gestisce al fine di verificare l'osservanza interna al regolamento
L'autorità di controllo	▪ il Garante della Privacy, la Guardia di Finanza e gli Organismi preposti

Il titolare del trattamento

Il Regolamento Europeo all'art. 4 definisce il **titolare del trattamento** (*data controller*) come

"***la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali***".

Si tratta di una figura già prevista nella normativa della Direttiva 95/46/CE ed è in pratica quel soggetto che, coincidendo solitamente con la più alta gerarchia aziendale, **dà le indicazioni fondamentali sul trattamento dei dati**. Non è, quindi, colui che gestisce i dati, ma è colui che **prende le decisioni più importanti** in merito, decidendo il perché e il come gestire il trattamento dei dati personali.

Il responsabile del trattamento

Il **responsabile del trattamento** (*data processor*) è
"*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Già prevista nella Direttiva Europea del 1995, tale figura si configuri in **un soggetto esterno all'azienda** (e quindi distinto dal titolare del trattamento), solitamente identificabile nei fornitori di servizi. Non a caso il legislatore europeo ha previsto esplicitamente che tra il titolare e il responsabile del trattamento debba stipularsi un **contratto di designazione**.

L’incaricato al trattamento dei dati

L’Incaricato del trattamento, è
"*la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile*".

Questa definizione già ci invita ad una prima e ben precisa considerazione: a differenza della figura del Titolare e di quella del Responsabile, l’Incaricato **può essere soltanto una persona fisica** e non anche una persona giuridica. Il secondo requisito che emerge in maniera inequivocabile dalla disposizione è che, per essere qualificata come Incaricato al compimento delle operazioni di trattamento, la persona fisica **deve ricevere apposita autorizzazione**. Pertanto, a differenza del Titolare, ma in modo speculare al Responsabile, l’Incaricato non assume tale veste in conseguenza ad uno stato di fatto, bensì solamente a seguito di espressa designazione.

Il responsabile protezione dati
(Il Data Protection Officer)

Chi può essere nominato DPO?

Un **soggetto interno** alla struttura del titolare o del responsabile del trattamento (es. un dipendente).

Un **soggetto esterno** alla struttura del titolare o del responsabile del trattamento che opera in base a un contratto di servizi.

Quali caratteristiche deve avere il DPO?

«*Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*».

OBBLIGO DI NOMINA DELLA FIGURA DEL DPO

Amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;

Tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati SU LARGA SCALA;

Tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici o di dati relativi a condanne penali.

La filosofia di fondo: Responsabilizzare

"Accountability e Responsability"

Accountability significa che, in forza del Regolamento, il titolare del trattamento deve mettere in atto **misure tecniche e organizzative** adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è stato effettuato conformemente al Regolamento.

Per «essere in grado di dimostrare» è bene redigere il Registro dei trattamenti dei dati anche quando non è obbligatorio.

Il Registro del trattamento

Definizione

Il Registro del trattamento è un nuovo strumento introdotto dal Regolamento Europeo per consentire alle autorità di controllo competenti di monitorare le attività di trattamento dei dati personali effettuate dal Titolare o dal Responsabile del trattamento sotto la propria responsabilità.

Forma

Il Registro del trattamento è da tenersi in forma scritta (anche in formato elettronico),

e va esibito all'autorità di controllo (Garante, Guardia di finanza ecc.) in caso di verifiche.

Finalità

«*Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere, un registro delle attività di trattamento effettuate sotto la sua responsabilità.*

Il **registro delle attività di trattamento** è previsto dall'art. 30 del R.E. che **lo rende obbligatorio** per le imprese o organizzazioni con più di 250 dipendenti e in tutti i casi in cui il **trattamento dei dati personali presenta un rischio per i diritti e le libertà** dell'interessato, o includa il trattamento di categorie **particolari di dati personali**

La tenuta del registro è utile per una **completa ricognizione e valutazione dei trattamenti svolti e quindi finalizzata anche all'analisi del rischio e ad una corretta pianificazione dei trattamenti**.

Si consiglia a tutti i titolari di trattamento di redigere il Registro, anche quando non obbligati, inserendo in esso ogni elemento utile, anche oltre a quelli minimi previsti dalle norme.

L’obbligo di notifica di una violazione dei dati personali

Si stabilisce l’obbligo per tutti i Titolari del trattamento di effettuare la **notifica della violazione all’autorità di controllo entro72** ore ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

Riepilogando gli obblighi e gli adempimenti:

- Obblighi di **informare e eventualmente raccogliere il consenso** al trattamento dei dati personali (quali dati, come trattati, per quanto tempo, ecc.);
- L'obbligo di **valutare il rischio** connesso al trattamento dei dati e l'impatto negativo sugli interessati in caso di violazione;
- La predisposizione di misure tecniche per garantire la sicurezza dei dati, cioè contro la possibilità di violazione (**data breach**), o di uso improprio
- Alcuni criteri generali per i sistemi informatici, per rispettare le norme: «**privacy by design**» e «**privacy by default**»
- L'**obbligo di notificare** agli interessati**,** entro le 72 ore successive, la violazione dei dati subita
- Redazione e mantenimento di un **«registro dei trattamenti**»

I nuovi diritti dell'Interessato

Diritto alla cancellazione (diritto all'oblio)

inteso come il diritto dell'interessato di ottenere dal titolare la cancellazione dei dati personali che lo riguardano in presenza di particolari condizioni

Diritto di limitazione di trattamento,

con cui l'interessato può chiedere una restrizione del trattamento

(ad es. la sola conservazione dei dati con esclusione di qualsiasi altro utilizzo)

Nella pratica:

- **Obblighi organizzativi e burocratici.** Si consiglia di adempiere questi obblighi collaborando attivamente con l'assistenza clienti offerta da **Italsoluzioni** così da predisporre documenti standard per raccolta consenso degli interessati, predisporre informative sulla privacy, tenere il registro dei trattamenti, ecc.

- **Misure di sicurezza informatiche** che non riguardano specificatamente la parte applicativa di Business, bensì **l'infrastruttura informatica su cui Business viene utilizzato: si tratta di misure e configurazioni di tipo sistemistico**, legate all'uso dei sistemi operativi, dei database, delle reti. **Italsoluzioni** offre una attività di consulenza che saprà dare consigli/indicazioni in questa materia, indicando o impostando le configurazioni più opportune.

- **Funzionalità arricchite di Business Cube** che consentono meglio agli utenti di gestire i dati personali nel solco dei principi generali stabiliti dal GDPR.

Nella pratica:

Ricordando proprietà già esistenti in Business o apportando nuovi aggiornamenti introdotti per adeguare Business a quanto previsto dal GDPR:

Potenziamento password

- Potenziamento Gestione autenticazione login
- Cambio periodico (già presente). Tempo di inattività + ripristino password. Numero tentativi falliti
- Impossibilità di usare le ultime «10» pw

Gestione Operatori

- Ogni operatore entra in Business con propria password (già presente)
- Abilitazione a Ditte e a programmi definiti dall'Amministrator (già presente)
- Formazione sul blocco utente da inserire quando si rende necessario e comunque ad ogni allontanamento dal PC

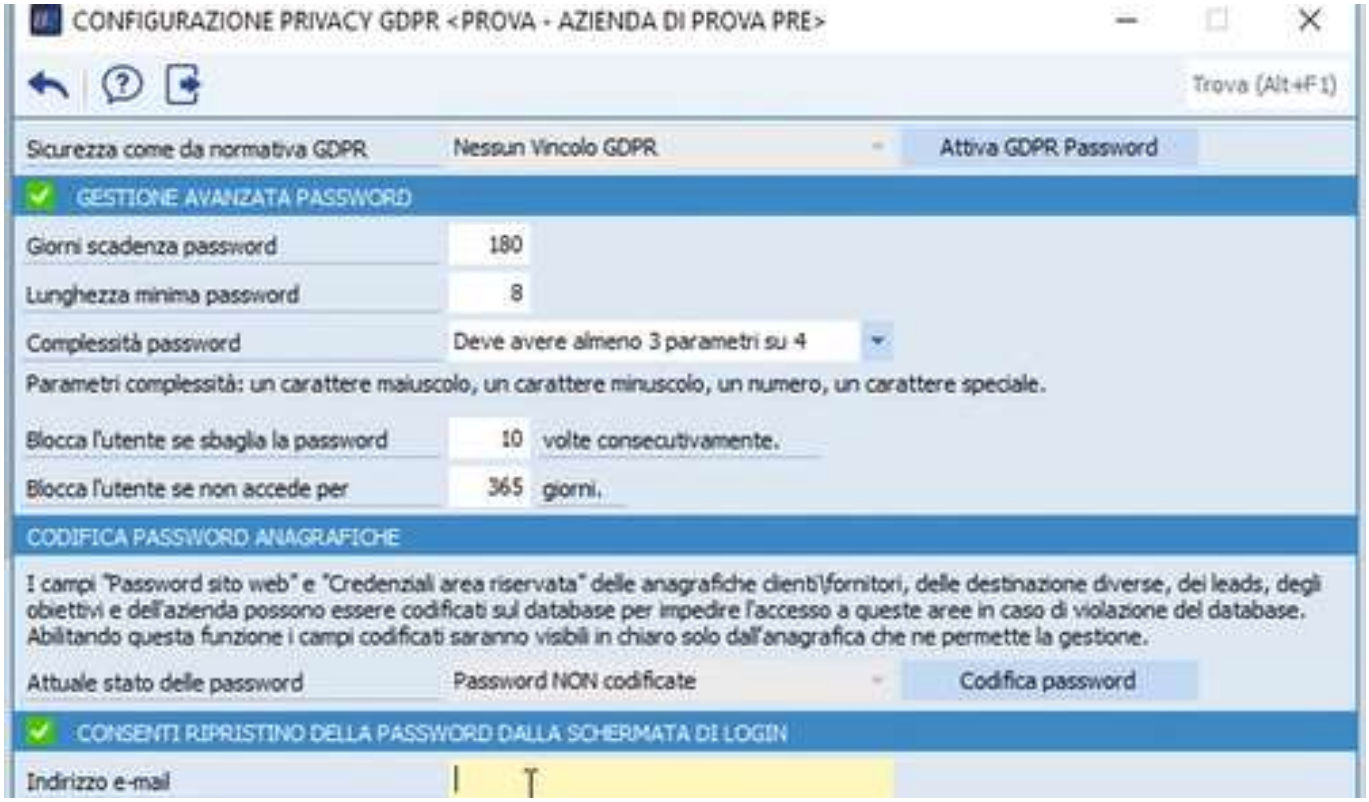
Potenziamento log

- Potenziamento log su modifica ai dati da parte degli operatori o da procedure (inserimento, modifiche chiare su tabelle dati personali)
- Log di accesso e disconnessione a Business e ai singoli programmi

Funzione di anonimizzazione

- Consente di creare un Database di Business anonimizzato

ITALSOLUZIONI



Con il supporto ai clienti, Italsoluzioni offre:

Uno studio atto ad ottenere un quadro completo delle attività di trattamento dei dati per finalità, categorie dei dati e degli interessati.

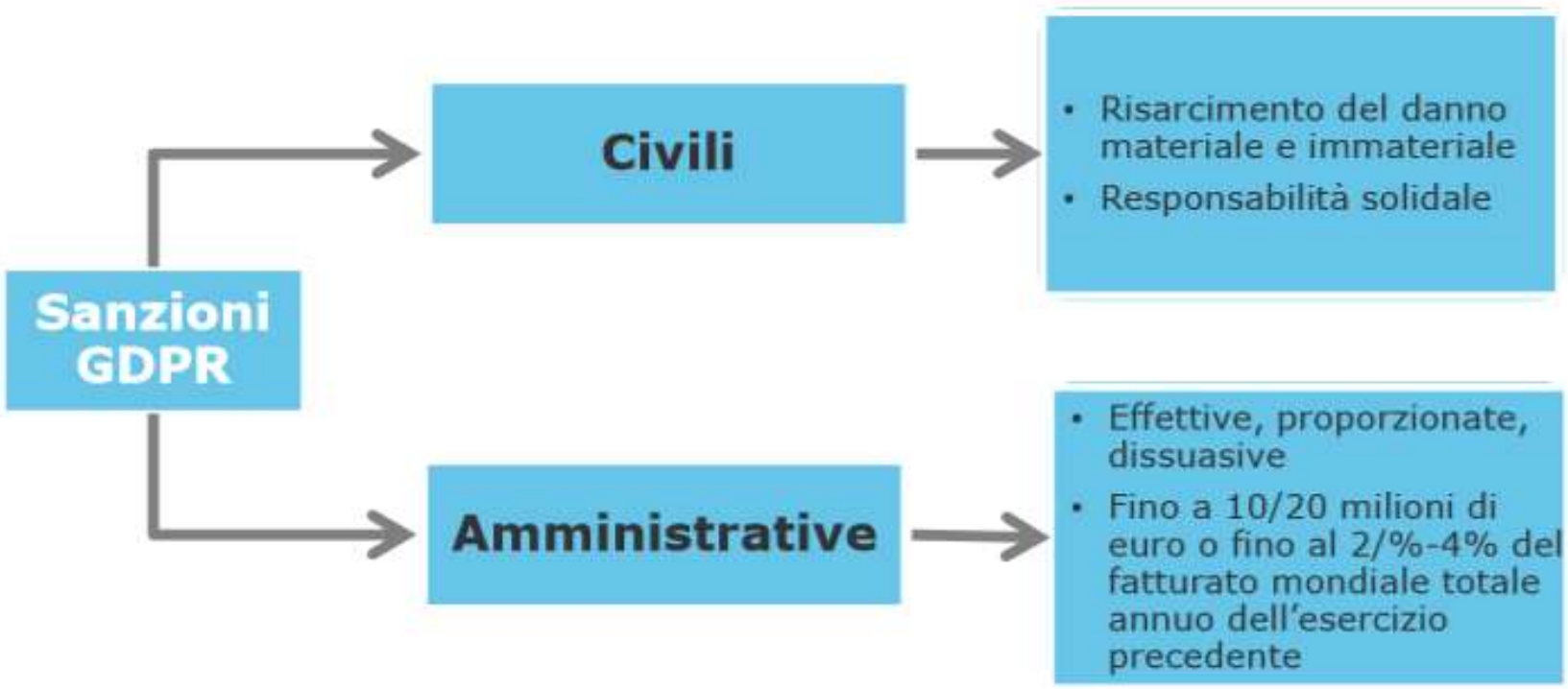
Produzione delle diverse informative e raccolta del consenso dove necessario

Intervento e adeguamento dei dispositivi informatici e delle procedure

Redazione del Registro dei trattamenti con relative valutazioni di impatto e analisi dei rischi ecc.

Pianificazione delle attività di controllo, istruzione e formazione periodica del personale, aggiornamento e adeguamento della documentazione con cadenza annuale.

Il Nuovo impianto sanzionatorio



Le sanzioni amministrative pecuniarie

1. Le violazioni agli obblighi in capo alle imprese (20 articoli su 49) sono punite fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo.

Ad esempio:

- ✓ la violazione dell'obbligo di tenuta del registro dei trattamenti;
- ✓ la mancata valutazione d'impatto DPIA (Data Protection Impact Analysis)
- ✓ l'omessa consultazione preventiva dell'Autorità;
- ✓ l'omessa notifica di data breach;
- ✓ l'omessa nomina del DPO;
- ✓ l'omessa adozione di misure di sicurezza adeguate.

Le sanzioni amministrative pecuniarie

2. Gli altri 29 articoli puniscono fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo la violazione dei principi del regolamento e dei diritti degli interessati.

Ad esempio:

- ✓ I principi di base del trattamento, comprese le condizioni relative al consenso;
- ✓ I diritti degli interessati;
- ✓ I trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- ✓ l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

La presentazione la potrete visionare sul nostro sito:

www.italsoluzioni.com

Nella pagina «L'azienda» -«Area Clienti»

- GDPR E Fatturaz. elettronica

oppure

http://italsoluzioni.dyndns.org:8000/Fatturazione%20elettronica/

Provvederemo a recepire sulla documentazione ogni eventuale aggiornamento normativo

Grazie per l'attenzione

Lo staff di Italsoluzioni Srl rimane a vostra completa disposizione

ITALSOLUZIONI s.r.l. - Via Giuseppe Ungaretti, 7 – 14053 Canelli (AT)-
Tel 0141-831014
mail: info@italsoluzioni.com **sito: www.italsoluzioni.com**