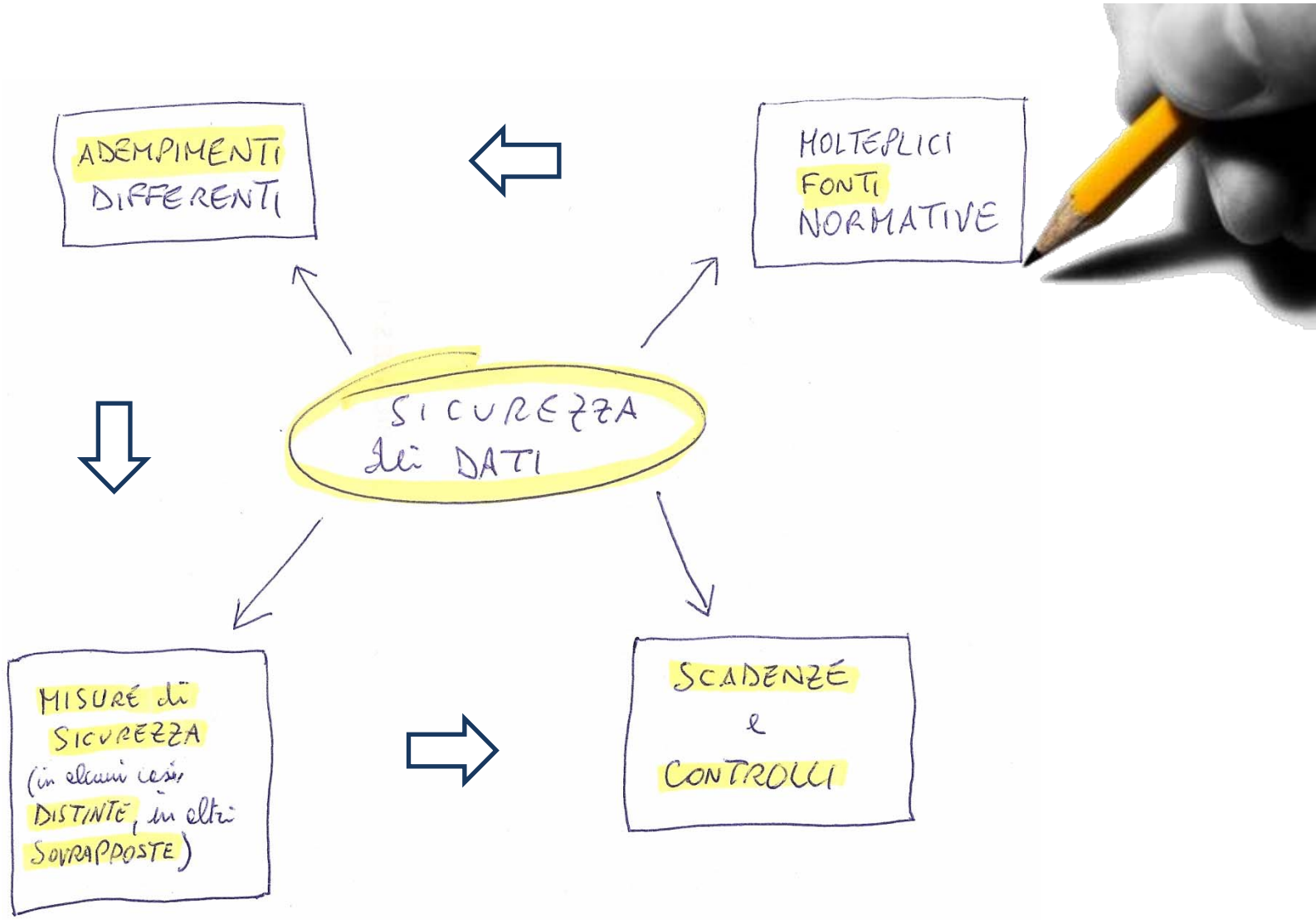
Sicurezza e continuità operativa

La normativa italiana e le linee evolutive europee sulla tutela dei dati

di
Riccardo Abeti

Abeti
Studio Legale


ADEMPIMENTI DIFFERENTI
MOLTEPLICI FONTI NORMATIVE
SICUREZZA dei DATI
MISURE di SICUREZZA (in alcuni casi DISTINTE, in altri SOVRAPPOSTE)
SCADENZE e CONTROLLI

Codice privacy

garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali

CAD

lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.

231

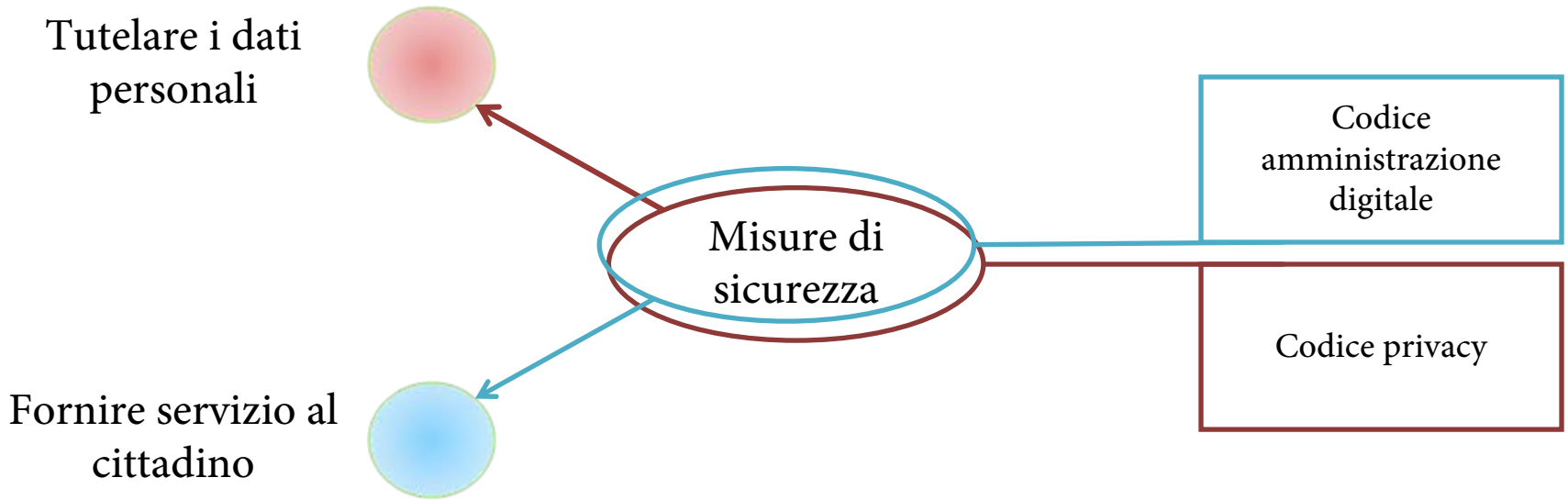
L'ente é responsabile per i reati commessi nel suo interesse o a suo vantaggio

Con il passare del tempo molte normative, pur avendo finalità differenti, convergono definendo un complesso frame di adempimenti e misure di sicurezza

Codice privacy	Redazione regolamento dati sensibili
CAD	Predisposizione Studio di Fattibilità Tecnica e sottoposizione dello stesso a DigitPA
231	Adozione modello organizzativo e gestionale

MISURE di SICUREZZA
(in alcuni casi DISTINTE, in altri SOVRAPPOSTE)

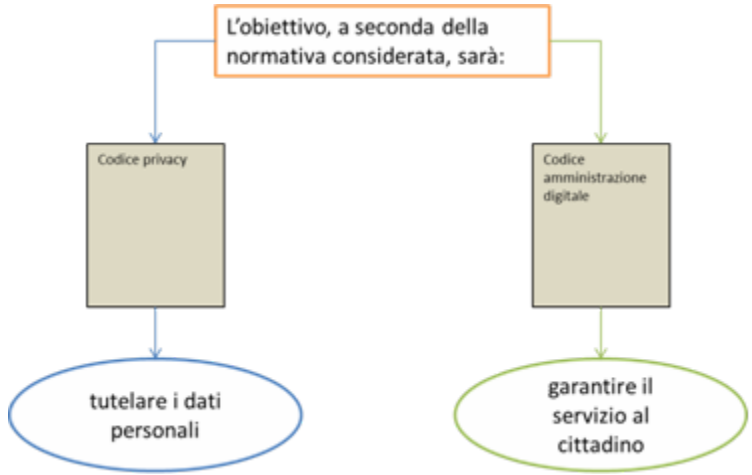
OBIETTIVO | MISURA | FONTE



ESEMPIO

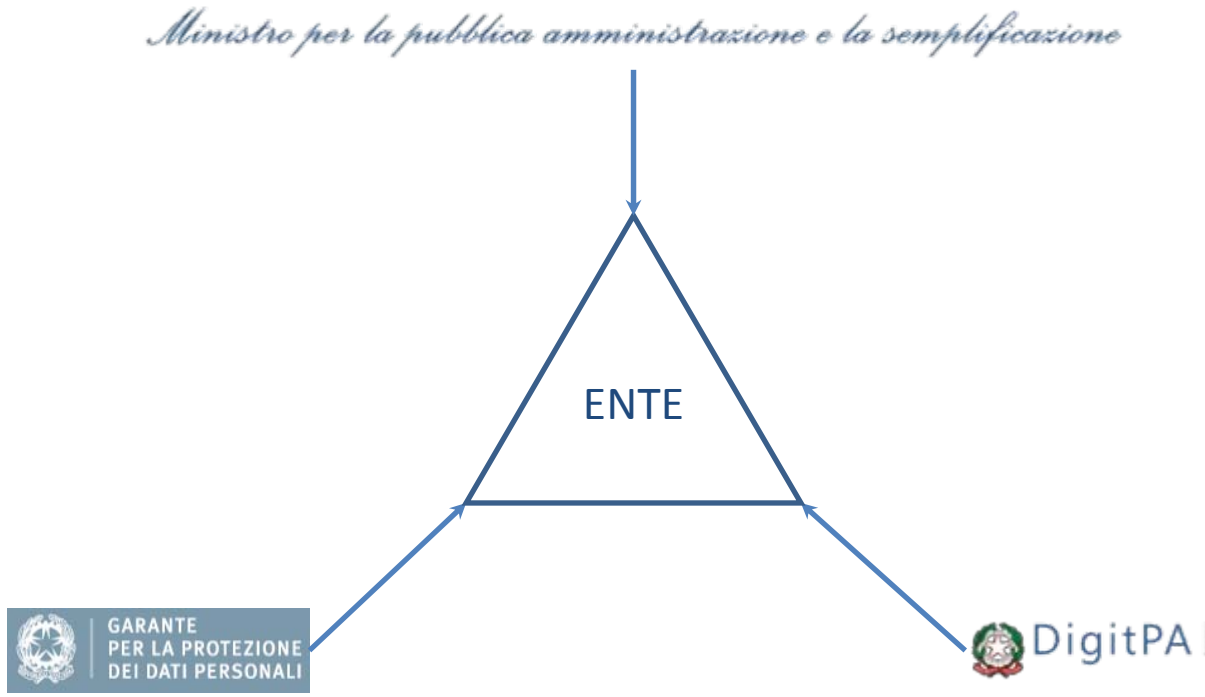
Secondo una diffusa definizione con la locuzione «continuità operativa»:
si intende la capacità dell'ente di continuare ad esercitare il proprio business a fronte di eventi avversi che possono colpirlo

In effetti, dotarsi di un Piano di Continuità Operativa può perseguire, come obiettivi complementari o come obiettivi principali, una serie di aspetti talvolta distanti da quello della definizione, ad esempio, guardando alle norme che ci interessano l'obiettivo sarà duplice, ovvero: garantire tutela ai dati personali (in termini di disponibilità ad esempio) e garantire il servizio al cittadino.



Abeti
Studio Legale

SCADENZE
&
CONTROLLI



riservatezza

integrità

tracciabilità

disponibilità

Vertraulichkeit

Verfügbarkeit

integrity

availability

confidentiality

Integrität

Abeti
Studio Legale

È importante l'adozione di misure di sicurezza come la cifratura o la separazione dei database ma anche il perseguimento dei principi di «necessarietà e pertinenza»

riservatezza

Art. 22, comma 6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

omissione degli elementi identificativi diretti

20. I dati sensibili e giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

misure che prevengano o traccino l'accesso abusivo

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati.

separazione fisica e logica

I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

cifratura

Paragrafo 6, scenario 2, punto 2 - *password* per l'apertura del file o in una chiave crittografica rese note agli interessati

chiavi crittografiche per apertura referto

Art. 50 bis CAD. Le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività

piano di continuità operativa

Punto 18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

operazioni di backup

Punto 23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

piano di ripristino

disponibilità

tracciabilità

Punto 1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

sistema di autenticazione

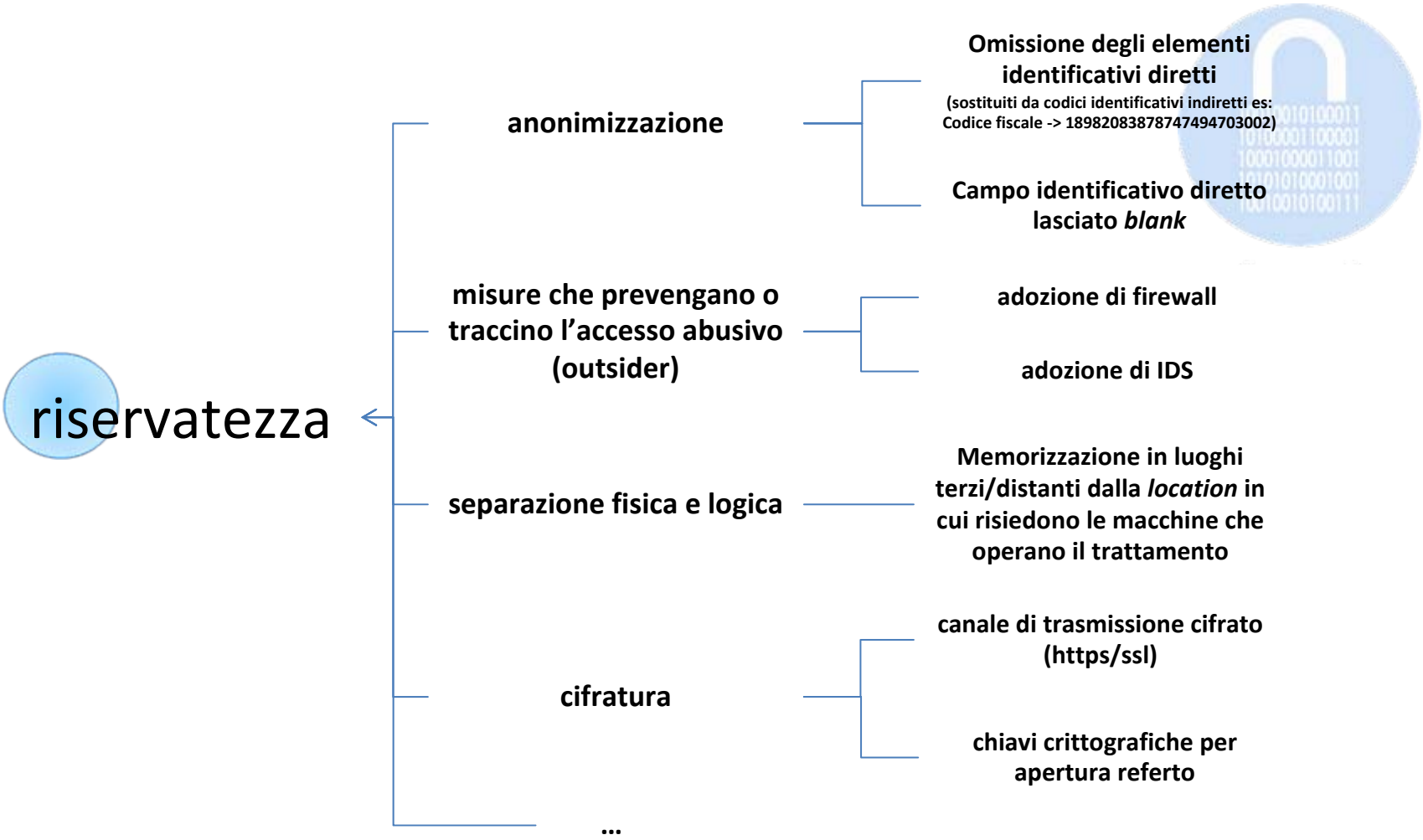
Punto 12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

sistema di autorizzazione

Abeti Studio Legale

Ambito di sicurezza	Misura di sicurezza	Rif.
riservatezza	misure che prevengano o traccino l'accesso abusivo al sistema(outsider)	Allegato B – punto 20
	separazione dei dati direttamente identificabili dai dati relativi alla salute e alla vita sessuale	Allegato B – punto 24
	cifratura	Codice privacy e Allegato B – punto 24
	temporanea inintelligibilità dei dati sensibili, anche ai soggetti autorizzati ad accedervi	Codice privacy – art. 22, comma 6
	trasmissione basata su standard crittografici con certificazione digitale dei sistemi che erogano i servizi	Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009
	cifratura file *system* e *database*	Linee guida per il trattamento di dati nell'ambito delle sperimentazioni cliniche di medicinali – 24 luglio 2008
	cancellazione automatica dati alla scadenza del periodo di retention	Provvedimento in materia di videosorveglianza - 8 aprile 2010 (3.3.1, lett. c)
	Distruzione dati identificativi dopo la raccolta (dopo la raccolta e successivamente all'eventuale verifica di attendibilità, ma sempre «senza ritardo»)	Linee guida in tema di trattamento dei dati per lo svolgimento di indagini di *customer satisfaction*
	sistemi per interrompere le procedure di spedizione di referti via email oppure rendano non disponibile l'informazione per la consultazione on-line (in caso di furto o smarrimento di credenziali)	Linee guida in tema di referti on-line - 19 novembre 2009

Ambito di sicurezza	Misura di sicurezza	Rif.
disponibilità	salvataggio dei dati	Allegato B – punto 18
	piano di ripristino	Allegato B – punto 23
	PCO (comprensivo di PDR)	Art. 50 bis del CAD
	I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale	Allegato B – punto 16
	aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti	Allegato B – punto 17
tracciabilità	sistemi di autenticazione	Allegato B – punto 1
	procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati	Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009
	adozione di sistemi di autenticazione forte	Linee guida in tema di referti on-line - 19 novembre 2009
	sistemi di autorizzazione	Allegato B – punto 12
	registrazione accessi da parte degli amministratori di sistema	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008
	adozione di audit-log	Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009



Abeti
Studio Legale

NUOVI ADEMPIMENTI

Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011
(Pubblicato sulla Gazzetta Ufficiale n. 127 del 3 giugno 2011)

5.1. Informazioni all'interessato*.
Le banche comunicano senza ritardo all'interessato le operazioni di trattamento illecito effettuate - sui dati personali allo stesso riferiti - dagli incaricati. Tale tempestiva informazione, infatti, in termini generali, può consentire all'interessato l'adozione di appropriate misure e, ove possibile, una minimizzazione dei rischi connessi alla violazione

5.2. Comunicazioni al Garante*.
Le banche comunicano tempestivamente al Garante –fornendo gli opportuni dettagli– i casi in cui risultino accertate violazioni, accidentali o illecite, nella protezione dei dati personali, purché di particolare rilevanza per la qualità o la quantità di dati coinvolti e/o il numero di clienti interessati, dalle quali derivino la distruzione, la perdita, la modifica, la rivelazione non autorizzata dei dati della clientela.

* Adempimenti introdotti sulla base di quanto disposto nella c.d. direttiva sulla e-privacy (2009/136/CE)

JUSTICE
European Commission

Commission proposes a comprehensive reform of the data protection rules

Date: 25/01/2012

Brussels, 25 January 2012 – The European Commission has today proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.

Press Pack

- Press Release
- Memo
- Press Conference with Vice President Reding: Commission proposes a comprehensive reform of EU data protection rules

Factsheets on data protection reform

- Why do we need an EU data protection reform? [594 KB]
- How does the data protection reform strengthen citizens' rights? [565 KB]
- How will the data protection reform affect social networks? [553 KB]
- How will the EU's data protection reform strengthen the internal market? [549 KB]
- How will the EU's data protection reform make international cooperation easier? [569 KB]
- How will the EU's data protection reform simplify the existing rules? [563 KB]
- How will the EU's data protection reform benefit European businesses? [554 KB]
- How will the EU's reform adapt data protection rules to new technological developments? [569 KB]

Public opinion surveys

- Attitudes on Data Protection and Electronic Identity in the European Union, June 2011 (Eurobarometer survey)
- Factsheets: Survey results by country

Commission Proposals on the data protection reform: legislative texts

- Communication
- Regulation [427 KB]
- Directive

Abeti
Studio Legale

Commission Proposals on the data protection reform: legislative texts

- Communication ...
- Regulation [427 KB] ...
- Directive ...

JUSTICE
European Commission

Uhjxodwhq

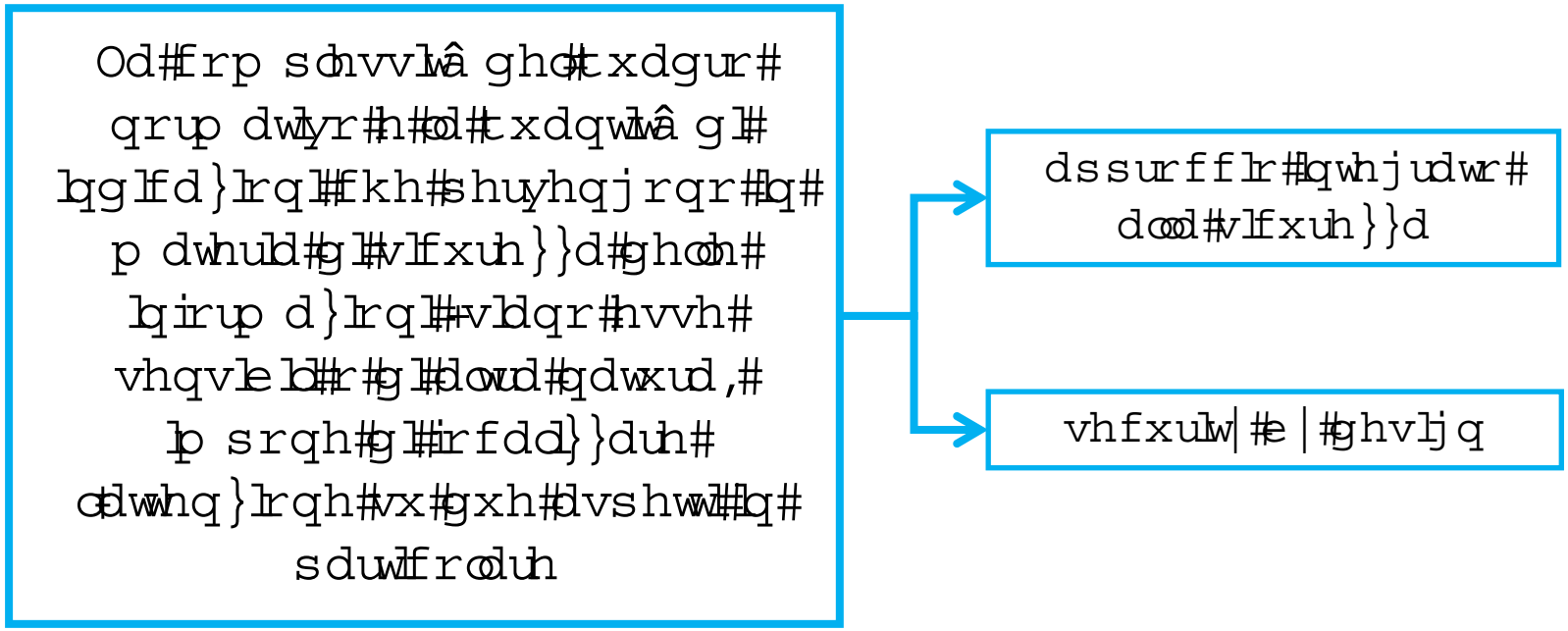
documentation (art. 28)

security by design (art. 23)

data breach notification (artt. 31-32)

Abeti
Studio Legale

Conclusioni



Abeti
Studio Legale

Grazie per l'attenzione.

Riccardo Abeti

Abeti
Studio Legale

Commission Proposals on the data protection reform: legislative texts

- Communication ...
- Regulation [427 KB] ...
- Directive ...

JUSTICE
European Commission

G luhfwlyh

Art. 27, comma 1
Responsabile e incaricato mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta e alla natura dei dati personali da proteggere (recupero).

La direttiva si limita a regolamentare il trattamento dei dati di carattere personale da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

Art. 27, comma 2
Responsabile e incaricato mettono in atto misure volte a:
a)vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento di dati personali (controllo dell'accesso alle attrezzature);
b)impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate (controllo dei supporti di dati);
c)impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (controllo della memorizzazione);
d)impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato di dati mediante attrezzature per la trasmissione di dati (controllo dell'utente);
e)garantire che le persone autorizzate a usare un sistema di trattamento automatizzato di dati abbiano accesso solo ai dati cui si riferisce la loro autorizzazione d'accesso (controllo dell'accesso ai dati);
f)garantire la possibilità di verificare e accertare a quali organismi siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati (controllo della trasmissione);
g)garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato dei dati, il momento dell'introduzione e la persona che l'ha effettuata (controllo dell'introduzione);
h)impedire che i dati personali possano essere letti, copiati, modificati o cancellati da persone non autorizzate durante i trasferimenti di dati personali o il trasporto di supporti di dati (controllo del trasporto);
i)garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati (recupero);
j)garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati (affidabilità) e che i dati personali memorizzati non possano essere falsati da un errore di funzionamento del sistema (autenticità).

Abeti
Studio Legale

Commission Proposals on the data protection reform: legislative texts

- Communication [...]
- Regulation [427 KB] [...]
- Directive [...]

JUSTICE
European Commission

Uhjxodwlrq

Articolo 23

Protezione fin dalla progettazione e protezione di default

1. Al momento di determinare i mezzi del trattamento e all'atto del trattamento stesso, **il responsabile** del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, **mette in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme al presente regolamento e assicuri la tutela dei diritti dell'interessato**.

2. Il responsabile del trattamento mette in atto meccanismi per garantire che **siano trattati**, di default, **solo i dati personali necessari per ciascuna finalità specifica del trattamento** e che, in particolare, la quantità dei dati raccolti e la durata della loro conservazione non vadano oltre il minimo necessario per le finalità perseguite. In particolare detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone.

Commission Proposals on the data protection reform: legislative texts

- Communication [...]
- Regulation [427 KB] [...]
- Directive [...]

JUSTICE

European Commission

documentation

Uhjxodwlrq

Articolo 28

Documentazione

1. Ogni responsabile del trattamento, […] conserva la documentazione di tutti i trattamenti effettuati sotto la propria responsabilità.
2. La documentazione contiene almeno le seguenti informazioni:
a) nome e coordinate di contatto del responsabile del trattamento[…];
b) nome e coordinate di contatto dell'eventuale responsabile della protezione dei dati;
c) finalità del trattamento, […];
d) descrizione delle categorie di interessati e delle pertinenti categorie di dati personali;
e) indicazione dei destinatari o delle categorie di destinatari dei dati personali, […];
f) se del caso, indicazione dei trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, […];
g) indicazione generale dei termini ultimi per cancellare le diverse categorie di dati;
h) descrizione dei meccanismi di verifica dell'efficacia delle misure di sicurezza adottate.
3. [...].
4. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano ai seguenti responsabili del trattamento e incaricati del trattamento:
a) persone fisiche che trattano dati personali senza un interesse commerciale,
oppure
b) imprese o organizzazioni con meno di 250 dipendenti che trattano dati personali solo accessoriamente rispetto alle attività principali.
5. [...]. […]

Abeti Studio Legale

Commission Proposals on the data protection reform: legislative texts

- Communication [...]
- Regulation [427 KB] [...]
- Directive [...]

JUSTICE
European Commission

Uhjxodwlrq

data breach notification

Articolo 31

Notificazione di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il responsabile del trattamento notifica la violazione all'autorità di controllo senza ritardo, ove possibile entro 24 ore dal momento in cui ne è venuto a conoscenza. Qualora non sia effettuata entro 24 ore, la notificazione all'autorità di controllo è corredata di una giustificazione motivata.

2. […] l'incaricato del trattamento allerta e informa il responsabile del trattamento immediatamente dopo aver accertato la violazione.

3. La notificazione di cui al paragrafo 1 deve come minimo:

a) descrivere la natura della violazione dei dati personali, compresi le categorie e il numero di interessati in questione e le categorie e il numero di registrazioni dei dati in questione;

b) […];

c) elencare le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione dei dati personali;

d) descrivere le conseguenze della violazione dei dati personali;

e) descrivere le misure proposte o adottate dal responsabile del trattamento per porre rimedio alla violazione dei dati personali.

4. Il responsabile del trattamento documenta la violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo. In essa figurano unicamente le informazioni necessarie a tal fine. […]

Abeti
Studio Legale

Commission Proposals on the data protection reform: legislative texts

- Communication [...]
- Regulation [427 KB] [...]
- Directive [...]

JUSTICE
European Commission

data breach notification

Uhjxodwrq

Articolo 32

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali rischia di pregiudicare i dati personali o di attentare alla vita privata dell'interessato, il responsabile del trattamento, dopo aver provveduto alla notificazione di cui all'articolo 31, comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 descrive la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 31, paragrafo 3, lettere b) e c).

3. Non è richiesta la comunicazione di una violazione dei dati personali all'interessato se il responsabile del trattamento dimostra in modo convincente all'autorità di controllo che ha utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati violati. Tali misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

4. [...].

5. [...].

6. [...].

Abeti
Studio Legale