Regolamento europeo 679/16 e Codice della Privacy

Regolamento 679 del 14 aprile 2016

- È entrato in vigore il 24 maggio 2016
- Gli enti devono **adeguarsi entro il 25 maggio 2018**
- **Obiettivo:** armonizzare le regole privacy dei vari stati e aggiornare le normative europee alla centralità del web

Situazione Italiana

14 maggio 2018 - Atto governo n. 22

Schema di decreto di adeguamento del Codice della privacy 196/2003

Obiettivo: Abrogare le disposizioni incompatibili con il regolamento UE

Dare attuazione alle disposizioni non immediatamente applicabili

Armonizzare la normativa italiana con il regolamento UE

Adeguare il sistema sanzionatorio

Sono mantenuti validi i **provvedimenti del Garante e le autorizzazioni**

Regolamento europeo 679/16 e Codice della Privacy

SI.NET Servizi Informatici

Sei in: Home » Leggi e Documenti » Attività non legislative

- Disegni di legge
- Leggi e decreti sul sito Parlamento
- Interrogazioni mozioni Sindacato ispettivo
- Attività non legislative
  - Elenco documenti
  - Ricerca
  - Ricerca testi pdf documenti
- Dossier di documentazione
- Ultimi atti pubblicati
- Statistiche
- Controllo dei rendiconti dei partiti politici

Attività non legislative

Atto del Governo sottoposto a parere parlamentare n. 22

Segui l'iter

XVIII Legislatura

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, 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 (regolamento generale sulla protezione dei dati)

Titolo breve: *Adeguamento normativa nazionale circa la protezione delle persone fisiche con riguardo al trattamento dei dati personali*

Testi disponibili dall'Archivio Legislativo

Atto del Governo sottoposto a parere parlamentare N. 22

Dossier di documentazione

Servizio del Bilancio

Nota di lettura - n. 13 (PDF)
Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, 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 (regolamento generale sulla protezione dei dati) (Atto del Governo n. 22)

Servizio Studi

Dossier - n. 18 (PDF)
L'adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679 - A.G. 22

Condividi

Versione per la stampa

La struttura del decreto

Art. 2 Il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento."; → **il codice della privacy non verrà abrogato, ma modificato**

Art. 2-*ter*

1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del Regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.
2. **La comunicazione (*dei dati*) tra titolari** è ammessa **quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico** e lo svolgimento di funzioni istituzionali **e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante**, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

La struttura del decreto

Art. 2-*sexies*

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi della lettera g), paragrafo 2, del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante.
2. *(Specifica i casi in cui è riconosciuto l'interesse pubblico)*

Art. 2-*septies* I dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo

La struttura del decreto

Art. 2-*octies* (Principi relativi al trattamento di dati relativi a condanne penali e reati)

1. il trattamento di dati relativi a condanne penali e a reati o a connesse misure di sicurezza (*è ammesso*)… solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento
2. In mancanza di tali delle predette disposizioni di legge o di regolamento, …le garanzie di cui al predetto medesimo comma sono individuate con decreto del Ministro della giustizia..
3. (*Specifica i casi in cui è riconosciuto l'interesse pubblico per cui è possibile trattare tale categoria di dati). A titolo d'esempio citiamo:*
    1. la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi e o dai regolamenti
    2. l'accertamento di responsabilità in relazione a sinistri
    3. l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto

La struttura del decreto

Art. 2-*novies* (Inutilizzabilità dei dati)

1. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 2-*decies* (limitazione ai diritti dell'interessato)

.. non possono essere esercitati

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al contro

La struttura del decreto

Art. 2-*duodecies* (diritti riguardanti le persone decedute)

1. I diritti .. riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.
2. ..
3. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

La struttura del decreto

Art. 2-*terdecies* (Attribuzione di funzioni e compiti a soggetti designati)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

La struttura del decreto

Art. 2-*quaterdecies* (Trattamento che presenta rischi specifici per l'esecuzione di un compito di interesse pubblico)

1. Con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati ai sensi dell'articolo 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

La struttura del decreto

Modifica all'art. 60 e dell'art.61 del Codice della Privacy

"Art. 60 (*Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale*)

1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale." .

Art.61

1. Il Garante promuove, …, l'adozione di regole deontologiche per il trattamento dei dati

La struttura del decreto

Modifica all'art. 80 del Codice della Privacy (SETTORE SANITARIO)

(Informazioni da parte di altri soggetti)

1. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento (*informative*), oltre a quanto previsto dall'articolo 79, possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di altri soggetti pubblici, diversi da quelli di cui al predetto articolo 79, operanti in ambito sanitario o della protezione e sicurezza sociale.
2. Le informazioni di cui al comma 1 è integrata sono integrate con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative effettuate per motivi di interesse pubblico rilevante che non richiedono il consenso degli interessati.";

La struttura del decreto

Modifica all'art. 99 del Codice della Privacy

"Art. 99 (*durata del trattamento*)

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

La struttura del decreto

introduzione dell'art. 111 bis del Codice della Privacy

"Art. 111-bis (*informazioni in caso di invio di curriculum*)

1. Le informazioni di cui all'articolo 13 del Regolamento e il consenso al trattamento non sono dovuti in caso di ricezione di curriculum spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Le informazioni vengono comunque fornite al momento del primo contatto successivo all'invio del curriculum.";

La struttura del decreto

introduzione dell'art. 132 ter del Codice della Privacy

Art. 132-ter (*sicurezza del trattamento*)

Il gdpr elimina le misure minime facendo riferimento alle misure adeguate

Alcune precisazioni:

5. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

La struttura del decreto

PROCEDIMENTO SANZIONATORIO (art. 158) – richiamo L. 689/1981

- Il garante, qualora riscontri una violazione avvia il procedimento
- L'ente può:
    - Attendere l'esito del procedimento
    - Presentare scritti e memorie entro 30 giorni
    - Pagare la metà della sanzione prevista per il reato ravvisato

SANZIONI PENALI (ART. 167)

1. Trattamento illecito dei dati
2. Comunicazione e diffusione illecita dei dati
    1. ai fini di trarre per me o per altri profitto
3. **Se vengono fornite notizie volutamente incomplete o false nell'ambito del procedimento del garante della privacy (6 mesi – 1 anno)**

PRIVACY E PUBBLICAZIONE DI DATI ON LINE

DIFFUSIONE DI DATI PERSONALI

Art. 11 D.LGS.196/2003

1) I dati personali oggetto di trattamento sono:

a) trattati in modo **lecito** e secondo correttezza;

b) raccolti e registrati per scopi **determinati**, espliciti e legittimi...

c) **esatti** e, se necessario, **aggiornati**;

d) **pertinenti, completi e non eccedenti** rispetto alle finalità per le quali sono raccolti e trattati;

e) **conservati** in una forma che consenta l'identificazione dell'interessato **per un periodo di tempo non superiore a quello necessario** agli scopi per i quali sono stati raccolti e trattati

2) I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

DIFFUSIONE DI DATI PERSONALI

Art. 19 c. 3 D.LGS.196/2003

DATI NON SENSIBILI O GIUDIZIARI

COMUNICAZIONE A
SOGGETTI PRIVATI, ENTI PUBBLICI
ECONOMICI E DIFFUSIONE
AMMESSE SOLO SE PREVISTE DA
NORMA DI LEGGE O REGOLAMENTO

DIFFUSIONE DI DATI PERSONALI

Art. 22 D.LGS.196/2003

DATI SENSIBILI O GIUDIZIARI

E' POSSIBILE TRATTARE SOLO I DATI **INDISPENSABILI** PER SVOLGERE ATTIVITA' ISTITUZIONALI CHE NON POSSONO ESSERE ADEMPIUTE DIVERSAMENTE (c. 3 e 5)

DATI IDONEI A RIVELARE LO STATO DI SALUTE

NON POSSONO ESSERE DIFFUSI (c. 8)

LE FINALITA' DELLA PUBBLICAZIONE ON LINE

- **Pubblicità**: garantire che atti e documenti amministrativi producano **effetti legali** al fine di favorire eventuali comportamenti conseguenti da parte degli interessati (es. pubblicità integrativa dell'efficacia, integrativa, notizia).

- **Trasparenza**: garantire la conoscenza delle informazioni al fine di assicurare un **ampio controllo sulle capacità delle PA** di raggiungere gli obiettivi nonché sulle modalità adottate per la valutazione del lavoro svolto dai dipendenti pubblici.

STRUMENTI E MODALITA' DI PUBBLICAZIONE

FINALITA' DIFFERENTI
Pubblicità, Trasparenza

DIFFERENTI STRUMENTI E MODALITA' DI PUBBLICAZIONE
(nel rispetto dei principi di necessità e proporzionalità)

DIFFUSIONE DI ATTI E DOCUMENTI DELLE PA

D. Lgs. 267/2000 (TUEL), art. 124: [PUBBLICITA' LEGALE]

Tutte le deliberazioni del comune e della provincia sono pubblicate mediante pubblicazione all'albo pretorio, nella sede dell'ente, per **quindici giorni consecutivi**, salvo specifiche disposizioni di legge

D. Lgs. 33/2013, art. 8: [TRASPARENZA]

I dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi della normativa vigente sono pubblicati **per un periodo di 5 anni**, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e quanto previsto dagli articoli 14, comma 2, e 15, comma 4.

Pubblicazione 15 gg (…) + Non ubiquità

POTREMMO ANDARE OLTRE QUESTE LIMITAZIONI?

(DIPENDE)

Art. 3 c. 3 L. 241/90: *“Se le ragioni della decisione risultano da altro atto dell'amministrazione richiamato dalla decisione stessa, insieme alla comunicazione di quest'ultima deve essere indicato e reso disponibile, a norma della presente legge, anche l'atto cui essa si richiama.”*

“Vista la nota prot. xy richiamata per relationem ex art. 3 c. 3 Legge 241/90 e da ritenersi parte integrante del presente atto”…

PROVV. GARANTE PRIVACY 19/04/07 (G.U. 25/5/07)

La circostanza secondo la **quale tutte le deliberazioni sono pubblicate** deve indurre l'amministrazione comunale a **valutare con estrema attenzione le stesse tecniche di redazione delle deliberazioni e dei loro allegati**. Ciò, **soprattutto quando vengono in considerazione informazioni sensibili** (…).

Può risultare ad esempio utile **menzionare tali dati solo negli atti a disposizione negli uffici (richiamati quale presupposto della deliberazione e consultabili solo da interessati e controinteressati)**, come pure menzionare delicate situazioni di disagio personale solo sulla base di espressioni di carattere più generale o, se del caso, di codici numerici.

GARANTE DELLA PRIVACY: PROVVEDIMENTI

Documento web	Data	Oggetto	Soggetto	Sanzione
3634427	09/10/14	Pubblicazione all'albo dati eccedenti finalità (Codice Fiscale, IBAN, dati anagrafici)	Comune	€ 4.000
3348446	10/07/14	Pubblicazione all'albo dati sanitari (TSO)	Comune	€ 10.000
3259444	19/06/14	Pubblicazione sul sito di dati relativi alla condizione di invalidità (dati sullo stato di salute)	Regione	
3280919	05/06/14	Pubblicazione all'albo di dati personali oltre 15 gg	Comune	€ 4.000
3281922	05/06/14	Pubblicazione all'albo di dati personali oltre 15 gg	Comune	€ 4.000
3393362	06/02/14	Pubblicazione sul sito di dati relativi a graduatoria disabili (dati sullo stato di salute)	Regione	€ 20.000
2554965	06/06/13	Pubblicazione sul sito elenco disabili (dati sullo stato di salute)	A.P.E.	
2192671	29/11/12	Pubblicazione sul sito elenco persone non autosufficienti (dati sullo stato di salute)	Comune	
1876679	23/02/12	Pubblicazione all'albo di dati personali oltre 15 gg	Comune	
1664456	07/10/09	Pubblicazione all'albo di dati di ricovero in strutture socio-assistenziali (dati sullo stato di salute)	Comune	

LE MISURE MINIME DI SICUREZZA ICT DELLE PUBBLICHE AMMINISTRAZIONI

NORME E CONTESTO

DIRETTIVA 1 AGOSTO 2015 Pres. Consiglio dei Ministri

- Adozione standard minimi di prevenzione e reazione ad eventi cibernetici.
- Ruolo di AgID (emanazione di regole, standard e guide tecniche)
- Ruolo del Nucleo per la sicurezza cibernetica, del CERT nazionale e del CERT-PA (adozione iniziative per l'allineamento agli standard nazionali di riferimento)

MISURE MINIME DI SICUREZZA ICT PER LE PA (26 APRILE 2016)

- Definizione Misure Minime Sicurezza ICT
- ABSC -> AgID Basic Security Control(s)

CIRCOLARE 18 aprile 2017 , n. 2/2017

- Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

PIANO TRIENNALE PER L'INFORMATICA NELLA PA

- Indicazioni in tema di sviluppo della sicurezza cibernetica delle PA.
- In attesa dell'emanazione da parte del Dipartimento della Funzione Pubblica delle Regole Tecniche per la sicurezza ICT delle Pubbliche amministrazioni proposte da AgID

I SOGGETTI COINVOLTI

Agenzia per l'Italia Digitale

CERT-PA (Computer Emergency Response Team Pubblica Amministrazione)

Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del C.A.D., ovvero, in sua assenza, il dirigente allo scopo designato

Rappresentante legale della struttura

L'OBBLIGO DI LEGGE

CIRCOLARE 18 aprile 2017 , n. 2/2017

Entro il 31/12/2017

L'OBBLIGO DI LEGGE

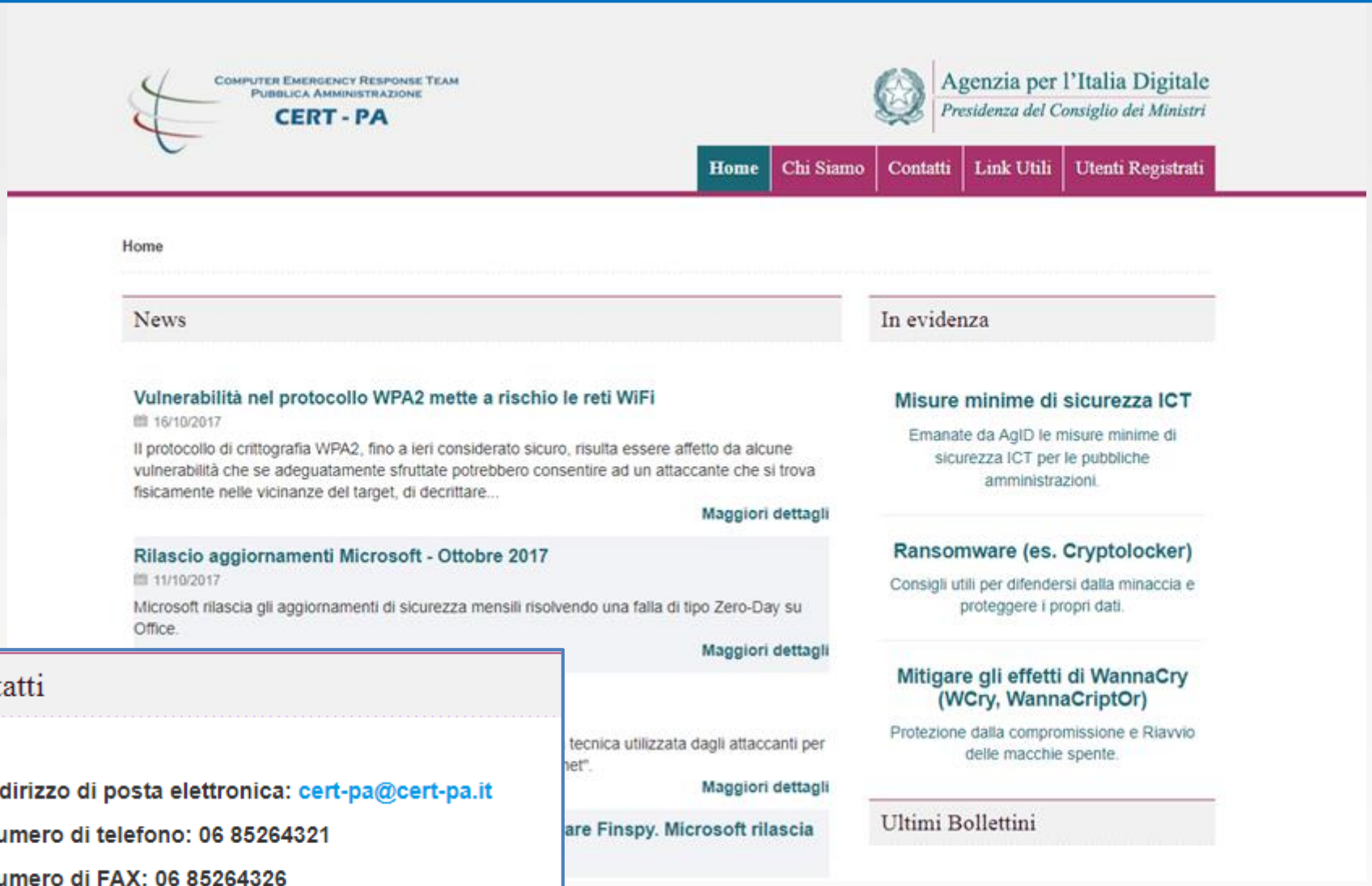
CIRCOLARE 18 aprile 2017 , n. 2/2017

In caso di incidente informatico

INVIO INSIEME ALLA SEGNALAZIONE DELL'INCIDENTE INFORMATICO

CERT-PA

https://www.cert-pa.it/



Contatti

- **Indirizzo di posta elettronica: cert-pa@cert-pa.it**
- **Numero di telefono: 06 85264321**
- **Numero di FAX: 06 85264326**

GDPR – violazione dati personali

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il titolare del trattamento dovrà comunicare eventuali violazioni dei dati personali (*data breach*) all'Autorità nazionale di protezione dei dati.
Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

GDPR – violazione dati personali

SI.NET Servizi Informatici

COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento**.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice.
Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

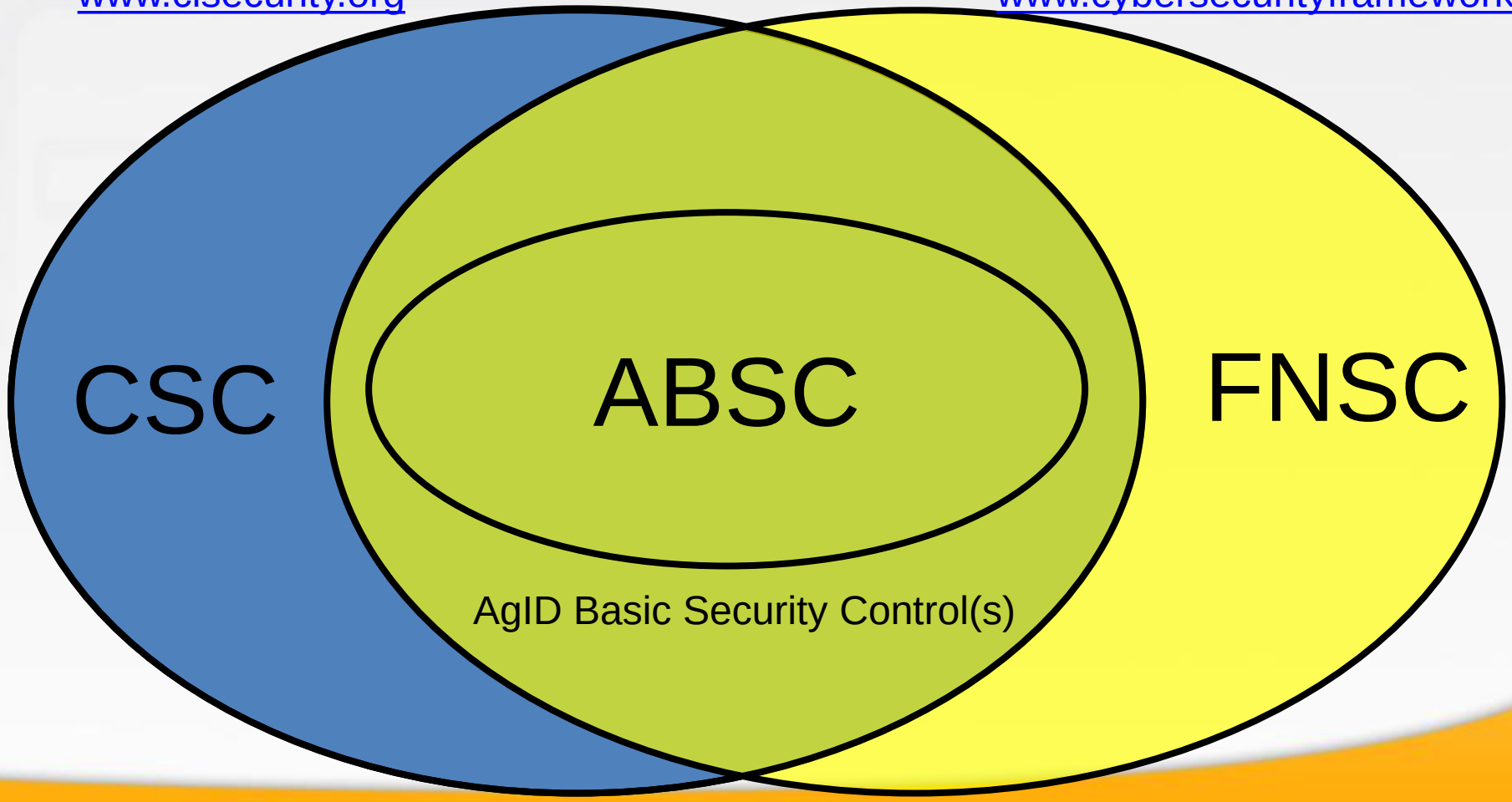
L’OBBLIGO DI LEGGE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	

RIFERIMENTI DI SICUREZZA

Critical Security Controls for
Effective Cyber Defense
(Center for Internet Security)
www.cisecurity.org

Framework Nazionale
Sicurezza Cibernetica
(CIS La Sapienza)
www.cybersecurityframework.it



CLASSI DI MISURE DEI CONTROLLI

ABSC 1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC 2: INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

CLASSI DI MISURE DEI CONTROLLI

ABSC 3: PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

CLASSI DI MISURE DEI CONTROLLI

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC 8: DIFESE CONTRO I MALWARE

CLASSI DI MISURE DEI CONTROLLI

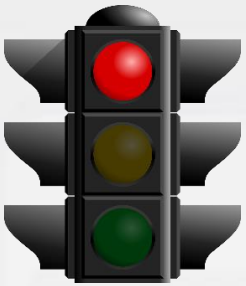
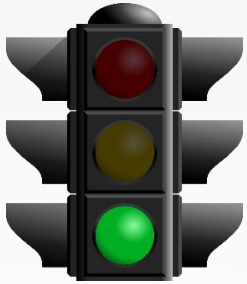
ABSC 10: COPIE DI SICUREZZA

ABSC 13: PROTEZIONE DEI DATI

CLASSI DI MISURE DEI CONTROLLI

ABSC_ID #			Descrizione	FNSC	Min.	Std.	Alto
1	1	1	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	ID.AM-1	X	X	X
		2	Implementare ABSC 1.1.1 attraverso uno strumento automatico	ID.AM-1		X	X
		3	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	ID.AM-1			X
		4	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	ID.AM-1			X
	2	1	Implementare il "logging" delle operazione del server DHCP.	ID.AM-1		X	X
		2	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	ID.AM-1		X	X
	3	1	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1	X	X	X
		2	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	ID.AM-1		X	X

3 LIVELLI DI SICUREZZA

	LIVELLO	DESCRIZIONE	M	S	A
	MINIMO	LIVELLO SOTTO IL QUALE NESSUNA AMMINISTRAZIONE PUO' SCENDERE: I CONTROLLI IN ESSA INDICATI DEBBONO RIGUARDARSI COME OBBLIGATORI	X	X	X
	STANDARD	BASE DI RIFERIMENTO NELLA MAGGIOR PARTE DEI CASI		X	X
	ALTO	OBIETTIVO A CUI TENDERE			X

Grazie per l'attenzione

aldo.lupi@sinetinformatica.it

Per seguire l'innovazione nella PA:

www.sinetinformatica.it

www.sinetinformatica.it/twitter

www.sinetinformatica.it/facebook