



# Smart Hospital & Mobile Health 4.0

**Covid-19: One Year after International Webinar/Tutorial From  
Hospital to Community and Home Care**

How Digital Health and Telemedicine  
can support the challenge against the Pandemic

March 12-13, 2021

Tecnologie digitali personali e social media

**Sicurezza e privacy dei dati medici:  
GDPR e vaccinazioni**

Giovanni Casiraghi (NewMicro)

D.LGS. 65/2018

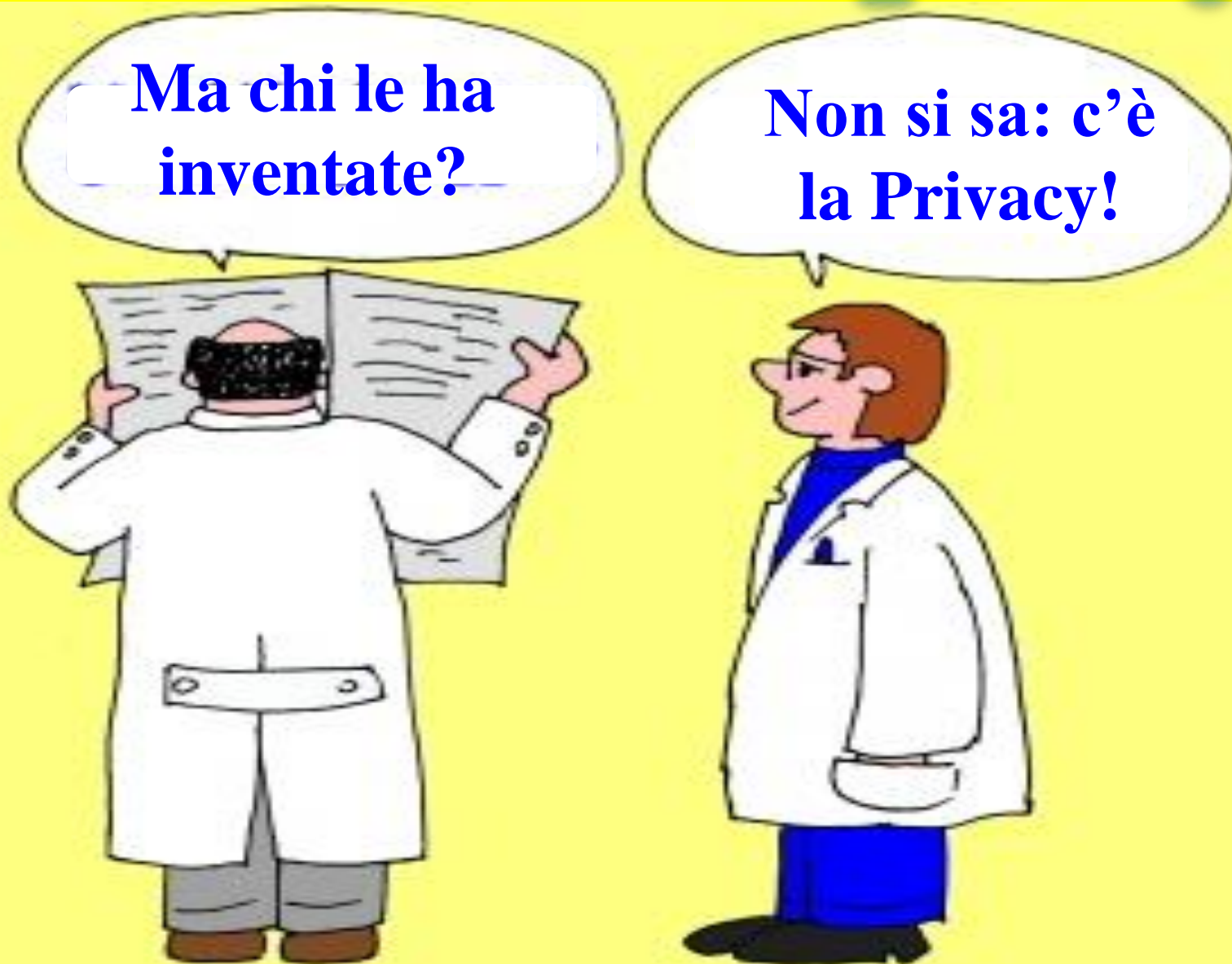
REGIONE DEL VENETO

# TRANSFORMATION



# Digitalizzazione First

# Nuove norme sulla privacy



# La Legislazione “di Recepimento”

Tutte le leggi “europee” prevedono

Vocabolario  
Definizione  
del  
significato  
dei termini  
utilizzati

Corsi di  
Formazione  
specifici  
sulla legge

valutazione  
dei rischi e  
modalità di  
segnalazione

L81/2008

L196/2003

679/2016

L190/2012

# GDPR - Regolamento (UE) 679/2016 - Le Parole

**Registri**

**RPD-DPO**

**Informativa**

**Titolare del  
Trattamento**

**DPIA**



**Big Data  
Data Breach**

**Diritti dei cittadini**

**Accountability**

**Privacy by Default e by Design**



# GDPR - Regolamento (UE) 679/2016



**Privacy personale** Gli individui hanno il diritto di:

- Accedere ai propri dati personali
- Correggere errori nei propri dati personali
- Cancellare i propri dati personali
- Contestare l'elaborazione dei propri dati personali
- Esportare i dati personali



**Controlli e notifiche** Le aziende saranno tenute a:

- Proteggere i dati personali con misure di sicurezza appropriate
- Segnalare alle autorità le violazioni dei dati personali
- Ottenere consenso appropriato per l'elaborazione dei dati
- Conservare la documentazione dettagliata sull'elaborazione dei dati



**Criteri di trasparenza** Le aziende sono tenute a:

- Fornire avvisi chiari sulla raccolta dati
- Evidenziare gli scopi dell'elaborazione e i casi di utilizzo
- Definire i criteri di conservazione e di eliminazione dei dati



**IT e formazione** Le aziende saranno tenute a:

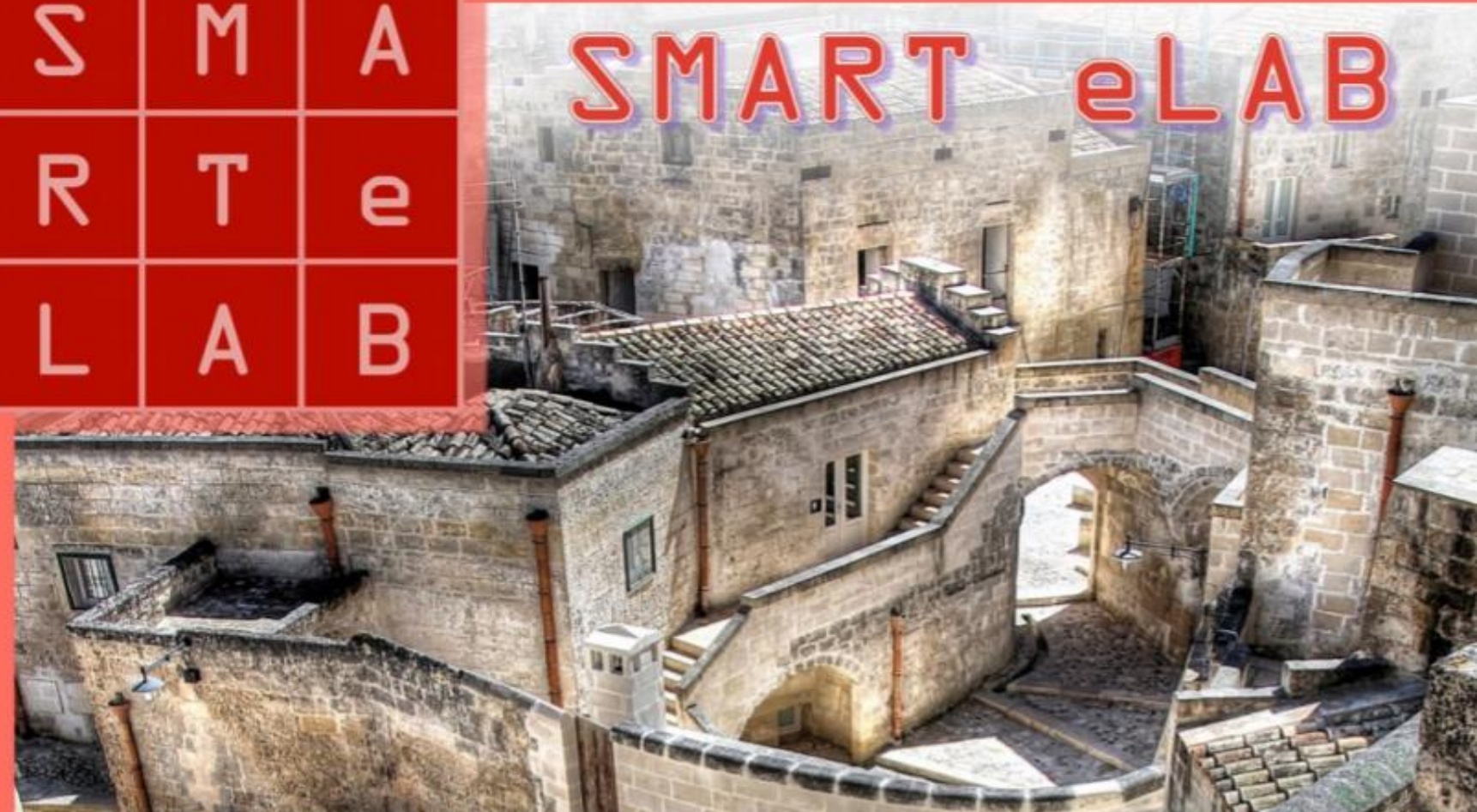
- Formare personale e dipendenti che si occupano di privacy
- Controllare e aggiornare i criteri relativi ai dati
- Avvalersi di un responsabile della protezione dei dati (se necessario)
- Creare e gestire contratti fornitore conformi

S M A

R T e

L A B

SMART eLAB



# Smart & Mobile Health '20

## Smart e Social Media in Sanità

7° Workshop/Tutorial Nazionale di Aggiornamento

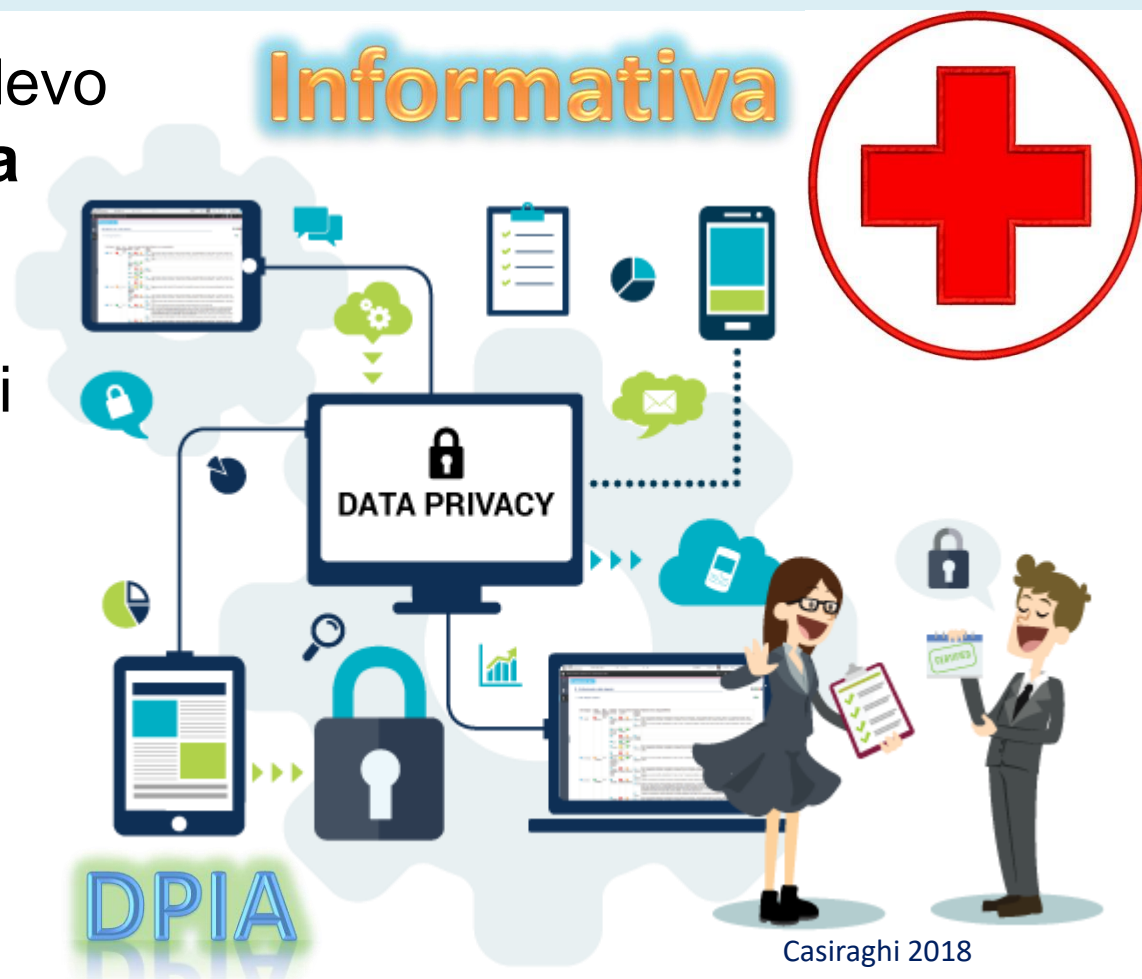
29 Gennaio 2020, Milano

Via Duccio di Boninsegna, 21 - Sala Conferenze (Piano Terra)

In area sanitaria la grande novità è il **venir meno dell'obbligo di consenso** quando i dati sono trattati per finalità di diagnosi e cura (art. 2-septies del Codice privacy emendato dal D. Lgs.101/2018 in combinata lettura con l'art. 9 GDPR).

**Meno burocrazia** (non devo chiedere il consenso), **ma molto più complessa** concettualmente, perché obbliga ad analizzare tutti i processi di trattamento per capire architettura e fondamento normativo.

**In sostanza è la finalità (dati) che comanda, e che guida e declina le prescrizioni a valle.**





# Fascicolo Sanitario Elettronico



## Personale



No consenso alla consultazione per finalità di studio e ricerca medica e di programmazione dei servizio sanitario. Ovviamente Il mancato consenso non pregiudica il diritto all'erogazione della prestazione sanitaria.

**decreto legge «Rilancio» n. 34/2020**, Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19. (20G00052) (GU Serie Generale n.128 del 19-05-2020 - Suppl. Ordinario n. 21)

# *Ancora su WA: Le ricette*





## L'informativa dovrà quindi contenere (sempre precisati):



i **dati di contatto** del titolare del trattamento, del DPO (*Data Protection Officer*) e, se nominati, del suo rappresentante sul territorio europeo del responsabile. L'interessato deve essere messo nelle condizioni di identificare chiaramente e di poter contattare i soggetti a cui spetta il trattamento dei propri dati personali (e a cui spetta garantirne la legittimità).

la **base giuridica** del trattamento. Le condizioni di liceità su cui il trattamento si basa: consenso, interesse legittimo del terzo, interesse pubblico, ecc.) e le **finalità** (scopo della raccolta o dell'elaborazione dei dati);



i **destinatari** o le categorie di destinatari dei dati personali: a chi verranno comunicati i dati o con chi verranno condivisi, anche per poter effettuare un servizio richiesto dallo stesso interessato;

**trasferimento di dati personali a un paese terzo** (extra europeo) Se ve ne sia l'intenzione da parte del titolare del trattamento di conferirli ad un'organizzazione internazionale: bisogna far sapere all'interessato se i suoi dati verranno diffusi al di fuori del territorio dell'Unione Europea;

il **periodo di conservazione** dei dati o i criteri utilizzati per determinarlo: periodo che sarà strettamente correlato allo scopo perseguito con il trattamento. Quando le finalità saranno state raggiunte, i dati non potranno più rimanere in possesso del titolare.

Si tratta di una valutazione che non è sempre possibile fare con certezza a priori.



## L'informativa dovrà quindi contenere (sempre precisati):



**l'esistenza** di una **serie di diritti**, dell'interessato, che gli consentono di controllare e gestire consapevolmente il flusso dei propri dati, in particolare: a) diritto di **accesso** ai dati, b) il diritto di chiederne la **rettifica**, la **cancellazione**, o la **limitazione** del trattamento, c) il diritto di **opporvi** al trattamento, d) il diritto alla **portabilità** dei dati, e) il diritto di **revocare il consenso** al trattamento, in qualsiasi momento ed f) il diritto di **proporre reclamo** all'autorità di controllo. far conoscere all'interessato quali siano questi diritti è compito del titolare esattamente come procedere per esercitarli in concreto (oltre a procedure semplici ed efficaci per attuarli)

se la comunicazione dei dati personali sia un **obbligo** legale, contrattuale, o oppure un requisito necessario per la conclusione di un contratto, e se l'interessato abbia l'obbligo di fornire i dati oltre alle **conseguenze** dell'eventuale mancata comunicazione: il titolare quindi deve dire all'interessato se la raccolta di quei dati sia necessaria o meno per poter fornire un servizio o dare esecuzione a una richiesta rivolta dall'interessato stesso oppure se sia direttamente la legge ad imporla. Inoltre, occorre spiegare all'interessato cosa succede nell'ipotesi in cui lo stesso non voglia comunicare i dati richiesti (il che, per lo più, consisterà nell'impossibilità di fornire il servizio in oggetto).

la **profilazione**, o l'esistenza di un **processo decisionale automatizzato**, aggiungendo informazioni che consentano all'interessato di comprendere in cosa consista in pratica quel trattamento: quindi informazioni sugli strumenti utilizzati, sulla portata del trattamento effettuato, sulla diffusione dei dati che ne può conseguire ecc.





# CORONAVIRUS E PROTEZIONE DEI DATI



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

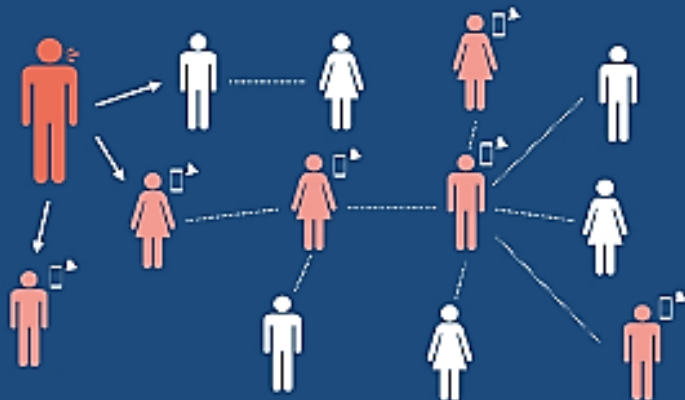


## CORONAVIRUS E PROTEZIONE DEI DATI

Raccolta delle **principali disposizioni adottate** in relazione allo stato di emergenza epidemiologica da **Covid-19** aventi implicazioni in materia di **protezione dei dati personali**

Uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19

Uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19



Casiraghi G -2021



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### COVID-19 e protezione dei dati personali



Treatment of data by local entities in the field of the health emergency



Treatment of data in the context of clinical trials and medical research in the field of the health emergency from Covid-19



Treatment of data in the context of health in the field of the health emergency



Treatment of data in the school context in the field of the health emergency



Treatment of data in the public and private work context in the field of the health emergency

# referti online

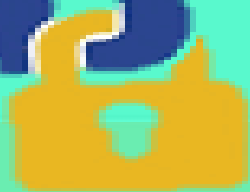


## procedura di self assessment

# DATA BREACH

Garante Privacy sanziona un policlinico, 20mila €

# RGPD



# 2020

## Violazioni di dati personali (Data Breach)



# L'oro dei big data

# CORTE DI CASSAZIONE

SECONDA PENALE  
SENTENZA 11959 /2020

Reati connessi all'informatica



Casiraghi G -2021

SESTA  
PENALE

SENTENZA 12094 /2020



# Bollettino: Azioni utili per contrastare l'esecuzione e la diffusione di malware

ID: CERT-PA-B006-191119

Data: 19/11/2019

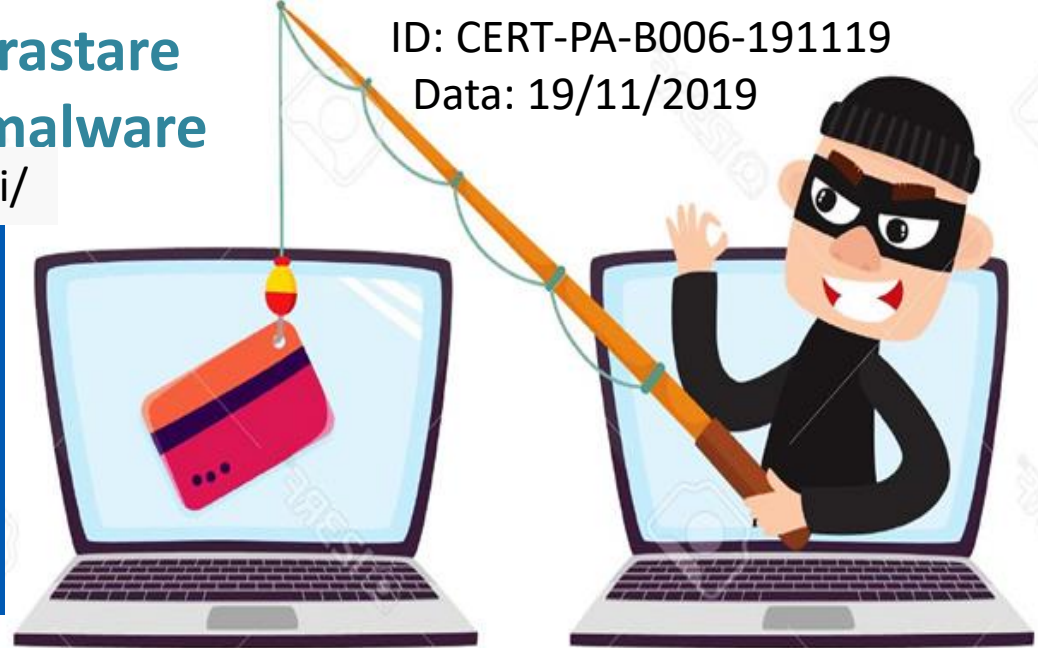
<https://www.cert-pa.it/category/bollettini/>



**AGID** | Agenzia per l'Italia digitale

Computer Emergency Response Team  
Pubblica Amministrazione

**CERT-PA**



Casiraghi G - 2021

**AVVERTENZE** Il documento ha lo scopo di fornire il quadro di riferimento degli scenari di minaccia rilevati dal CERT-PA, al fine di consentire tempestive valutazioni di impatto sui propri sistemi informativi e implementare le opportune misure di contrasto/contenimento dei rischi correlati.

Il CERT-PA, a fronte della sempre maggior diffusione di campagne miranti alla diffusione di malware attraverso l'utilizzo dei canali di posta ordinaria (PEO) e posta certificata (PEC) vuole suggerire in questo documento alcune configurazioni che è possibile applicare alle postazioni di lavoro per contrastare più efficacemente questi tipi di attacco.

<https://www.cert-pa.it/wp-content/uploads/2019/11/CERT-PA-B006-191119.pdf>

<https://www.cert-pa.it/pillole-informative/>

**Pillole Informative**

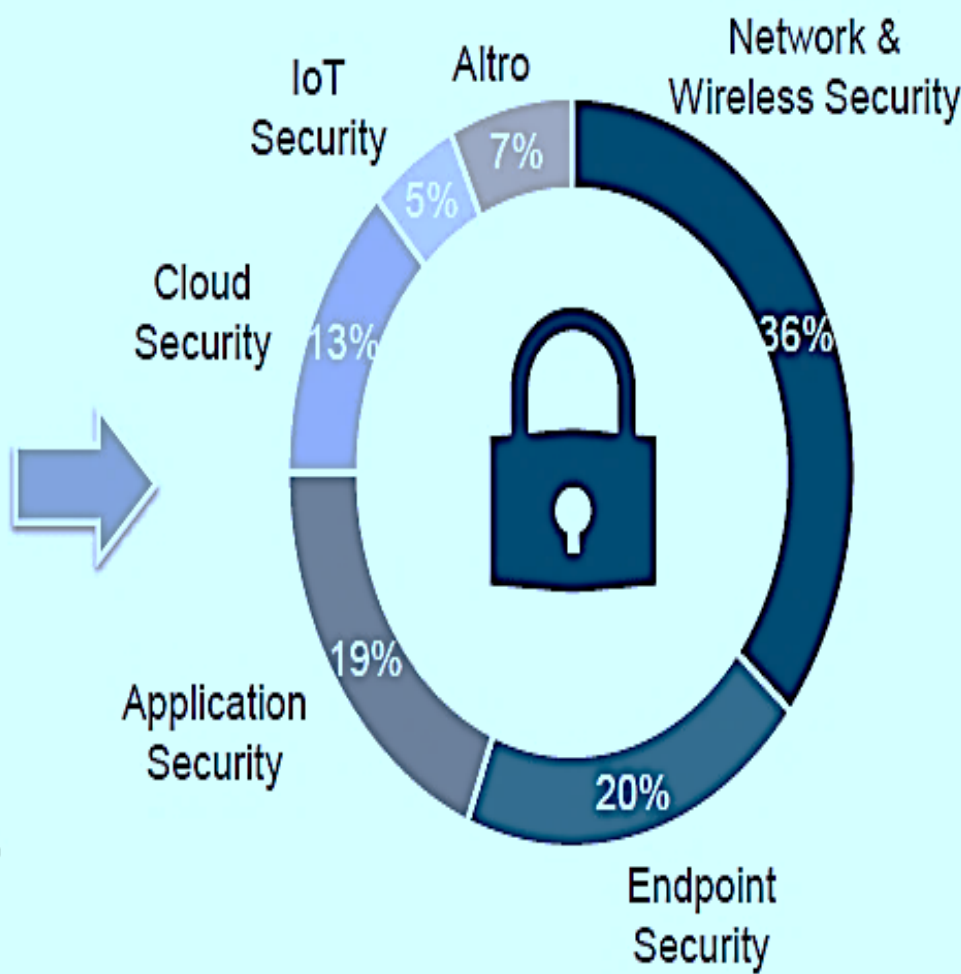
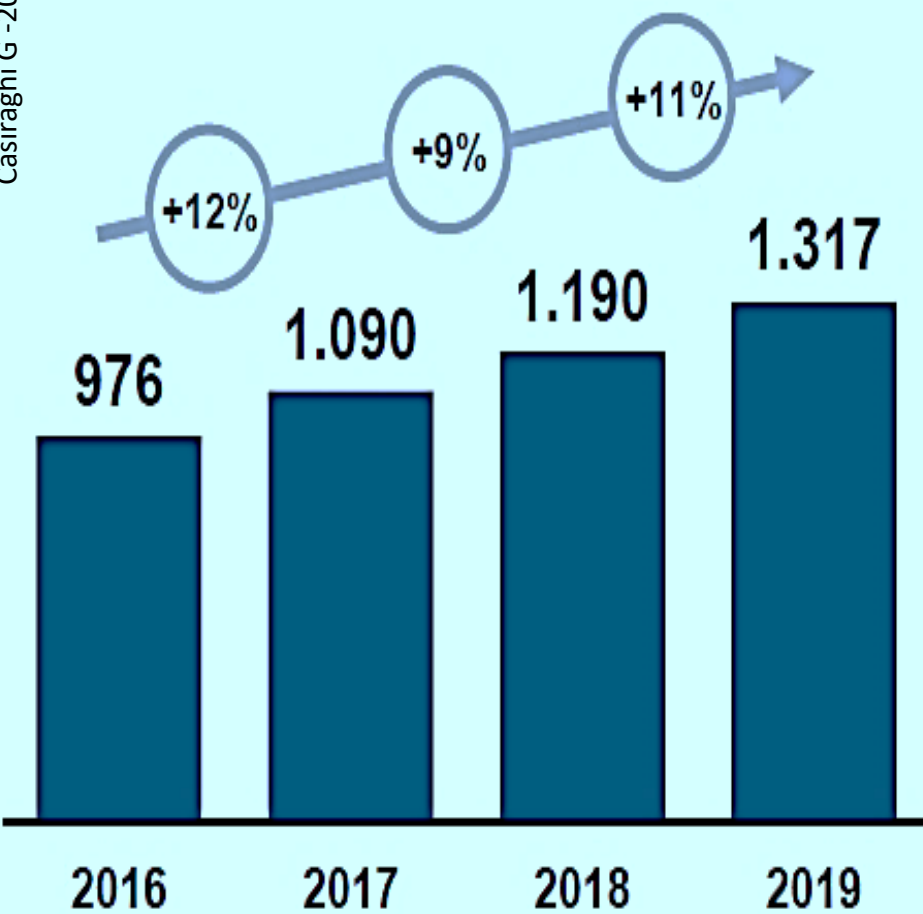
<https://www.cert-pa.it/wp-content/uploads/2018/10/Phishing-Cert-PA.pdf>

<https://www.cert-pa.it/wp-content/uploads/2018/10/criptovalute-finale.pdf>

<https://www.cert-pa.it/wp-content/uploads/2019/06/Data-Breach.pdf>

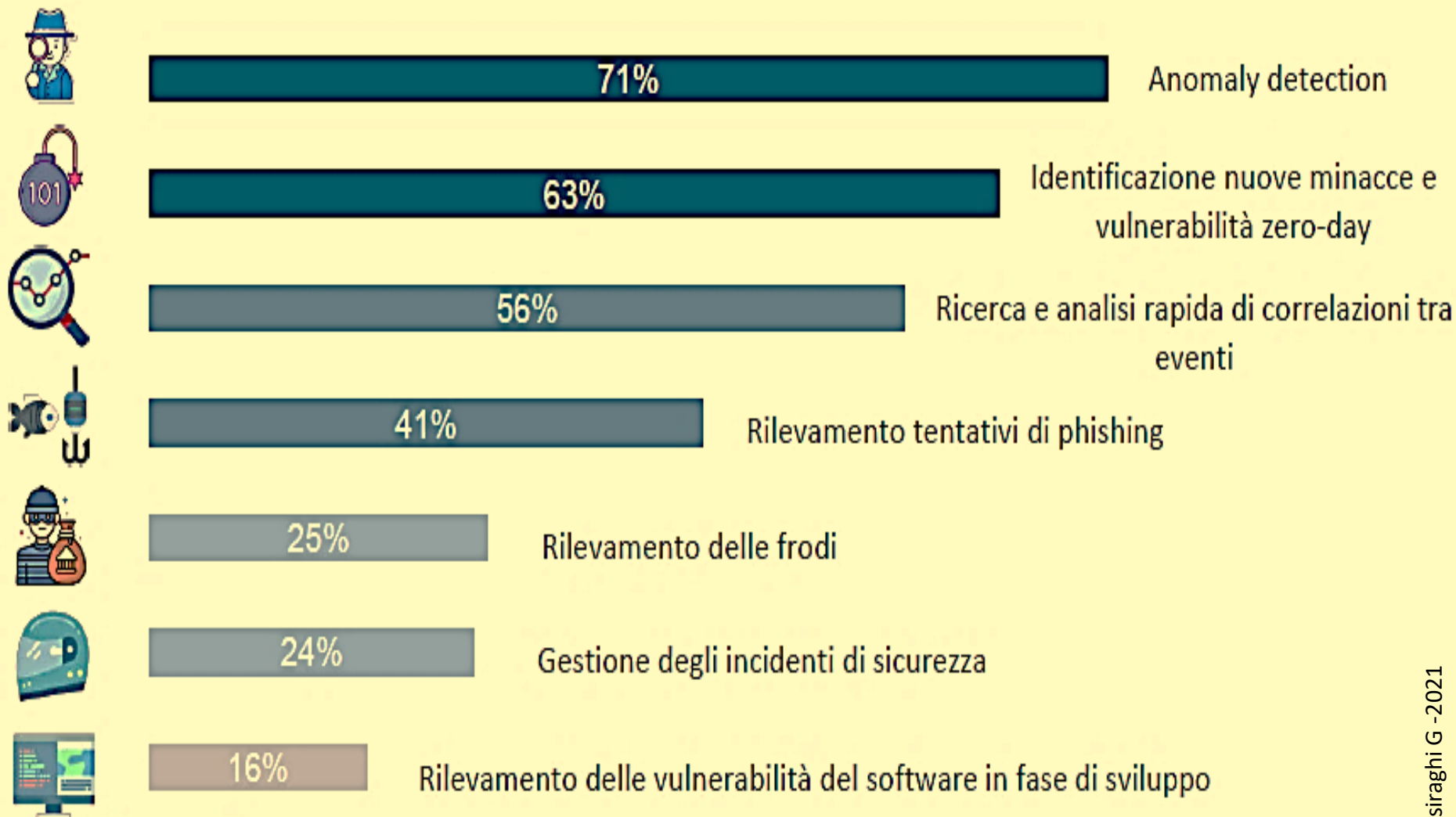


# Il mercato information security 2019



Campione: 698 organizzazioni italiane (dati in k€)

# Le funzionalità dell'AI in ambito security



Campione: 180 grandi imprese

# Ci salverà una App? Solo se conforme alla UNI/TR 11708



UNI/TR 11708 «Caratterizzazione delle App nel contesto della salute, benessere e stili di vita»

Un quadro di riferimento italiano per le App di eHealth/Wellness recepito ed in via di estensione in Europa



*Pier Angelo Sottile*  
[p.sottile@gmail.com](mailto:p.sottile@gmail.com)  
[psottile@heritageventures.eu](mailto:psottile@heritageventures.eu)

# Scenari Covid 19



ecdc

EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL





# Anagrafe Nazionale Vaccini


## Covid & Vaccinazioni





Gli operatori autorizzati a utilizzare il SIAVR sono quelli dotati di carta operatore SISS con i seguenti Ruoli:

1. Medico Medicina Generale  
Pediatrica
2. Medico Vaccinatore ASST
- 3. Medico Referente ASST**
4. Medico Referente ATS
5. Medico RSA
6. Infermiere coordinatore ASST
7. Infermiere coordinatore ATS
8. Infermiere vaccinatore
9. Farmacista ASST
10. Amministrativo ASST
11. Amministrativo coordinatore ASST
12. Direttore Sanitario ASST
13. Referente Regione Lombardia



### Medico Referente ASST

<b>Funzionalità SIAVR</b>	<ul style="list-style-type: none"> <li>• Gestione dell'Anagrafe Vaccinale</li> <li>• Erogazione Vaccini</li> <li>• Calendario e programmazione appuntamenti</li> <li>• Gestione Storico Vaccinale</li> <li>• Gestione Lotti e Magazzino</li> <li>• Statistiche</li> </ul>
<b>Ruolo applicativo SISS</b>	R.A. = 13 L1 = AO
<b>Credenziale estesa</b>	SPEC = VAC CAT = RESP

Fai clic sulla voce del ruolo per visualizzare la scheda di dettaglio relativa.



# *E la firma digitale?*

Come fare per...

Compilare il questionario pre-vaccinale?





# DALLA RELAZIONE 2018

La carente sicurezza dei dati e dei sistemi che li ospitano può rappresentare, in altri termini, **una causa di malasania**. La violazione delle regole essenziali di protezione dati può avere effetti deleteri nei processi medici, tanto più gravi ove quei processi incidano su aspetti qualificanti l'esistenza individuale: la nascita, la morte, la genitorialità".



La protezione dei dati è un **fattore determinante di efficienza sanitaria**, funzionale anche alla correttezza del processo analitico fondato su big data. Dall'esattezza dei dati utilizzati nel processo algoritmico dipende, infatti, l'"intelligenza" delle loro scelte, che tanto più in ambito diagnostico non possono tollerare errori.

# Horizon Europe: struttura preliminare



## Pilastro 1

Eccellenza scientifica

Consiglio europeo della  
ricerca

Azioni Marie Skłodowska-  
Curie

Infrastrutture di ricerca



## Pilastro 2

Sfide globali e competitività  
industriale europea

Poli tematici

- Sanità
- Cultura, creatività e società inclusiva
- Sicurezza civile per la società
- Digitale, industria e spazio
- Clima, energia e mobilità
- Prodotti alimentari, bioeconomia, risorse naturali, agricoltura e ambiente

Centro comune di ricerca (JRC)



## Pilastro 3

Europa innovativa

Consiglio europeo per  
l'innovazione

Ecosistemi europei  
dell'innovazione

Istituto europeo di  
innovazione  
e tecnologia

**Ampliare la partecipazione e consolidare lo Spazio europeo della ricerca**

Ampliare la partecipazione e diffondere l'eccellenza

Riformare e migliorare il sistema europeo di R&I



Commissione  
europea

Casiraghi G - 2021

UOMINI  
e  
MACCHINE



Protezione dati  
per un'etica del digitale

Atti del Convegno - 30 gennaio 2018

GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

DECRETO LEGISLATIVO 30 giugno 2003, n.196  
recante il "Codice in materia di protezione dei dati personali"  
(in S.O.n. 123 alla G.U. 29 luglio 2003, n. 174)



integrato con le modifiche introdotte dal

DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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)"  
(in G.U. 4 settembre 2018 n.205)

# DATA CRACY