Data governance e sicurezza

Sinergie fra GDPR e Circolare 285 di Banca d'Italia

Giancarlo Butti

Milano, Università degli Studi di Milano, 30 novembre 2017

Giancarlo Butti (LA BS7799), (LA ISO IEC 27001:2013), CRISC, ISM, DPO, CBCI, AMBCI

Master di II livello in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Mi occupo di ICT, organizzazione e normativa dai primi anni 80:
•analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
•consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni

Come divulgatore ho all'attivo:
• oltre 700 articoli su 20 diverse testate tradizionali e 7 on line
• 21 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
• 8 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT
• membro della faculty di ABI Formazione e docente presso altre istituzioni
• docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer in Banca di cui ho curato l'impianto ed il test finale
• relatore presso eventi di ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN…

Sono socio e proboviro di AIEA/ISACA (www.aiea.it – Associazione Italiana Information Systems Auditors), socio del CLUSIT (www.clusit.it – Associazione Italiana per la Sicurezza Informatica) e di BCI (www.thebci.org)

Partecipo ai gruppi di lavoro di ABI LAB sulla Business Continuity , Rischio informatico e GDPR, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su privacy, frodi, eidas, sicurezza dei pagamenti, SOC, di UNINFO sui profili professionali privacy, di ASSOGESTIONI su Privacy EU.
Fra i coordinatori di www.europrivacy.info.

BANCO BPM

Data governance

BANCO BPM

Definzioni

Data Governance is the exercise of decision-making and authority for data-related matters.

Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.

BANCO BPM

The DGI Data Governance Framework

ALLEGATO A
SISTEMI INFORMATIVI
4. Qualità dei dati e sicurezza informatica
Le procedure di raccolta, archiviazione ed elaborazione dei dati garantiscono il rispetto di elevati ***standard di qualità****; sono individuate tutte le informazioni rilevanti* ***(completezza)*** *e utili al calcolo dei rating* ***(pertinenza),*** *senza distorsioni*
sistematiche nei risultati indotte dai dati di input o dai processi di raccolta e integrazione ***(accuratezza)***.
E' definito uno ***standard aziendale di data policy*** *comprensivo dei controlli previsti e delle misure per trattare i dati mancanti o non soddisfacenti.*
Periodicamente, viene condotta una valutazione sul soddisfacimento di tale standard; nel tempo vengono fissati obiettivi sempre più stringenti in tema di qualità dei dati.
La banca individua le funzioni coinvolte nella raccolta dei dati e nella produzione delle informazioni; sono attribuiti ruoli e responsabilità per garantire una ordinata gestione dei dati, dei concetti statistici e del dizionario dati (c.d. "modello dati").
I dati acquisiti o rivisti con immissione manuale (ad esempio, registrazione dei questionari qualitativi, rettifiche di importi, correzione di una posizione per consentire l'associazione al relativo modello di valutazione, inserimento degli override) sono documentati; vengono registrati i dati precedenti la modifica, l'utente che ha rettificato, cancellato o aggiunto informazioni, e, nei casi rilevanti, le motivazioni degli interventi codificate per gruppi omogenei. Gli interventi manuali sono costantemente verificati, anche con appositi controlli nelle procedure di acquisizione, e, ove possibile, progressivamente sostituiti da procedure automatiche.
Viene tenuta traccia dei controlli effettuati e degli esiti, dei dati scartati o introdotti nelle varie fasi, delle informazioni mancanti, non plausibili, outlier o con forti discontinuità tra due periodi, delle posizioni escluse o non correttamente
associate a modelli di rating, dei risultati delle riconciliazioni con le procedure contabili e delle verifiche con archivi esterni.
E'attuata una politica di sicurezza atta a prevenire l'accesso ai dati da parte di soggetti non autorizzati e a garantire la loro integrità e disponibilità. Il piano di continuità operativa assicura, in caso di incidente, il recupero dei sistemi e degli archivi utilizzati per la misurazione del rischio di credito in tempi compatibili con le esigenze operative.

3. Compiti dell'organo con funzione di gestione

*-approva gli standard di **data governance**, le procedure di gestione dei cambiamenti e degli incidenti (ove del caso, in raccordo con le procedure del fornitore di servizi) e, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di business nonché con le strategie aziendali;*

Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013

BANCO BPM

IL SISTEMA DI GESTIONE DEI DATI

Il sistema di ***registrazione e reporting*** *dei dati è deputato a* ***tracciare tempestivamente tutte le operazioni aziendali e i fatti di gestione*** *al fine di fornire* ***informazioni complete e aggiornate*** *sulla attività aziendali e sull'evoluzione dei rischi. Esso assicura nel continuo* ***l'integrità, completezza e correttezza dei dati conservati e delle informazioni rappresentate****; inoltre, garantisce* ***l'accountability e l'agevole verificabilità*** *(ad es., da parte delle funzioni di controllo) delle operazioni registrate.*

In particolare, il sistema di gestione dei dati soddisfa i seguenti requisiti:

- ***la registrazione dei fatti aziendali*** *è* ***completa****,* ***corretta*** *e* ***tempestiva****, al fine di consentire la ricostruzione dell'attività svolta (1);*

-è definito uno ***standard aziendale di data governance****, che individua* ***ruoli*** *e* ***responsabilità*** *delle funzioni coinvolte nell'utilizzo e nel trattamento, a fini operativi e gestionali delle informazioni aziendali (2); in considerazione della loro rilevanza nel sistema informativo, sono definite le misure atte a garantire e a misurare la* ***qualità*** *(3), ad es. attraverso* ***key quality indicator*** *riportati periodicamente agli utenti di business, alle funzioni di controllo e all'organo con funzione di gestione;*

Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013

BANCO BPM

- la identificazione, la misurazione o la valutazione, il monitoraggio, la prevenzione o l'attenuazione dei ***rischi connessi con la qualità dei dati*** *fa parte del processo di* ***gestione dei rischi*** *(cfr. Capitolo 7); in caso di acquisizione o incorporazione di soggetti esterni, la due diligence comprende la valutazione dell'impatto dell'operazione sulle procedure di gestione e* ***aggregazione dei dati****; l'utilizzo di* ***procedure settoriali*** *(contabilità, segnalazioni, antiriciclaggio, ecc.) non compromette la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, il* ***sistema di gruppo*** *assicura l'integrazione tra le informazioni provenienti da tutte le componenti del gruppo;*
- nel caso di ricorso a un ***data warehouse aziendale a fini di analisi e reporting****, le procedure di estrazione dei dati, di trasformazione, controllo e caricamento negli archivi accentrati – così come le funzioni di sfruttamento dei dati – sono* ***dettagliatamente documentate****, al fine di consentire la verifica sulla* ***qualità dei dati****;*
- le procedure di ***gestione e aggregazione dei dati sono documentate****, con specifica previsione delle circostanze in cui è ammessa l'****immissione o la rettifica manuale di dati*** *aziendali,* ***registrando*** *data, ora, autore e motivo dell'intervento, ambiente operativo interessato e i dati precedenti la modifica;*

Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013

BANCO BPM

*- i processi di acquisizione di dati da **information provider esterni** sono documentati e presidiati;*
*- i dati sono conservati con una **granularità adeguata** a consentire le diverse analisi e aggregazioni richieste dalle procedure di sfruttamento;*
*- i rapporti prodotti espongono le principali **assunzioni** e gli eventuali **criteri di stima** adottati (ad es., nell'ambito del monitoraggio dei rischi aziendali);*
*- il sistema di reporting consente di produrre informazioni **tempestive** e di **qualità** elevata per l'autorità di vigilanza e per il mercato.*

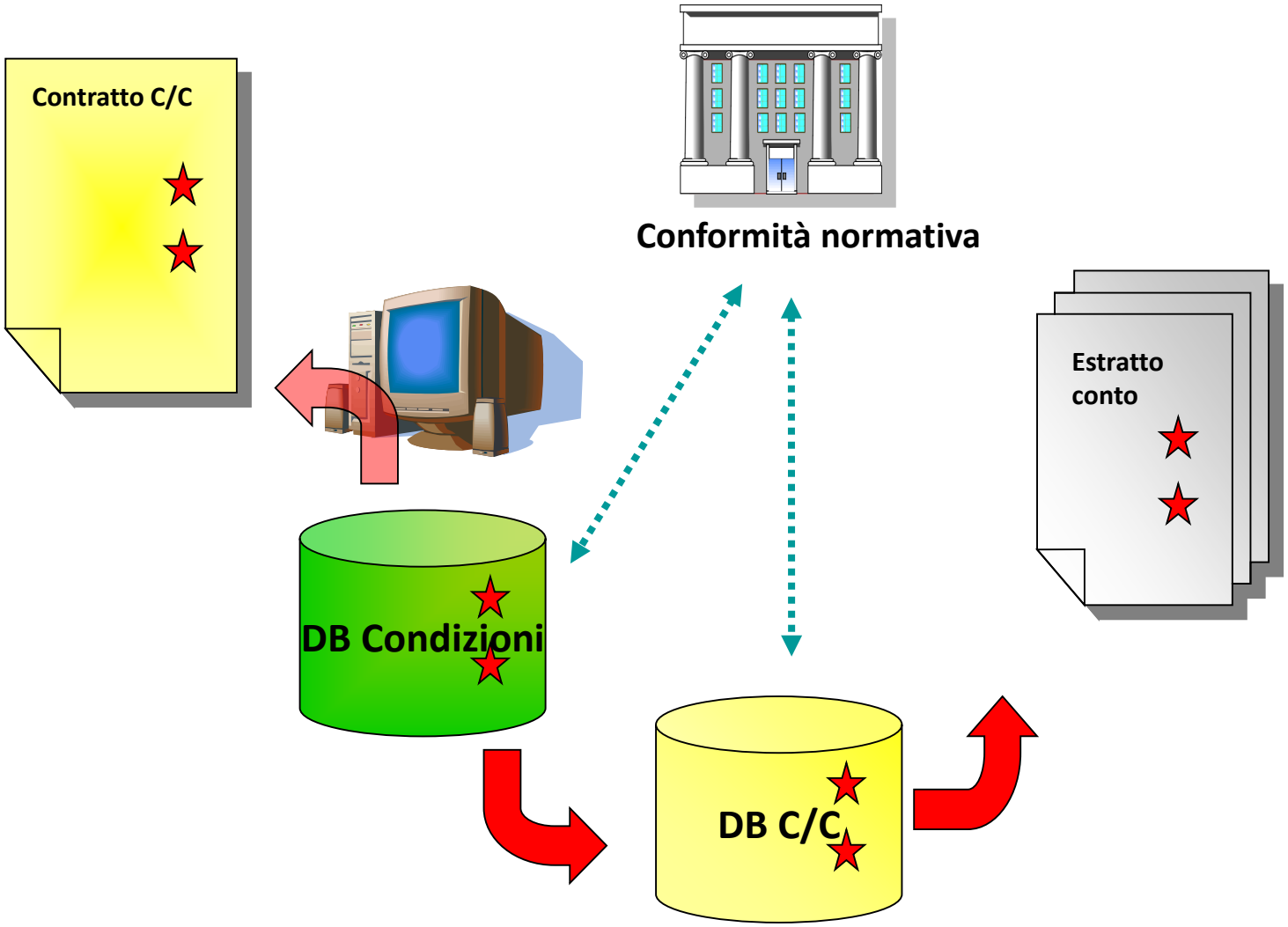
*(2) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capito I.5) individuano per i dati rilevanti (**informazione al mercato, segnalazioni all'Organo di Vigilanza, valutazione dei rischi**, ecc.) una o più figure aziendali responsabili di assicurare lo svolgimento dei controlli previsti e della validazione della qualità dei dati (c.d. "**data owner**"). Le procedure di aggregazione dei dati a fini di valutazione dei rischi aziendali sono sottoposte a validazione indipendente (ad es., da parte dell'internal audit).*

*(3) La qualità dei dati è valutata, in termini di **completezza** (registrazione di tutti gli eventi, operazioni e informazioni con i pertinenti attributi necessari per le elaborazioni), di **accuratezza** (assenza di distorsione nei processi di registrazione, raccolta e di successivo trattamento dei dati) e di **tempestività**.*

Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013

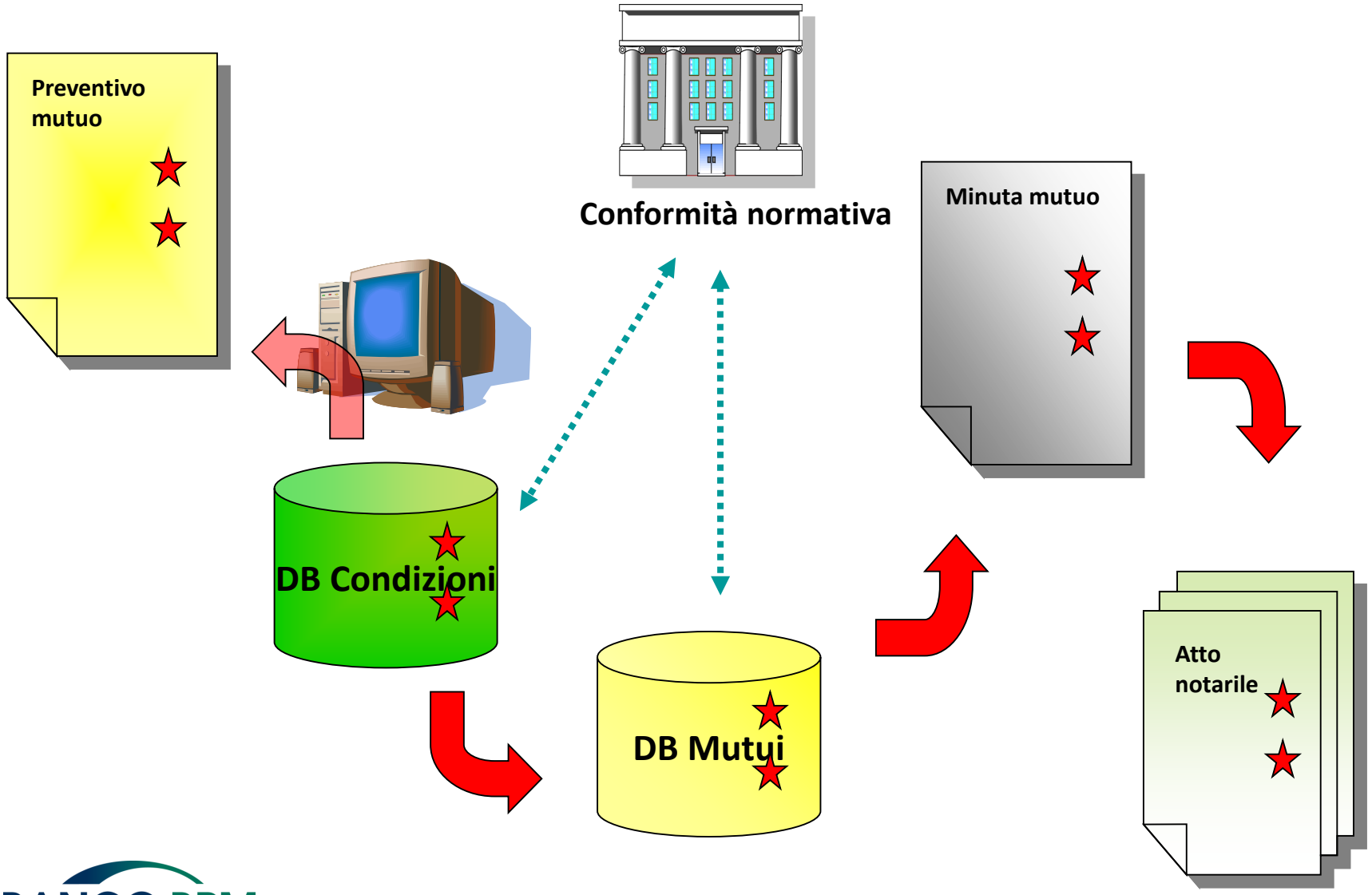
BANCO BPM

Processo esempio: Coerenza dati c/c



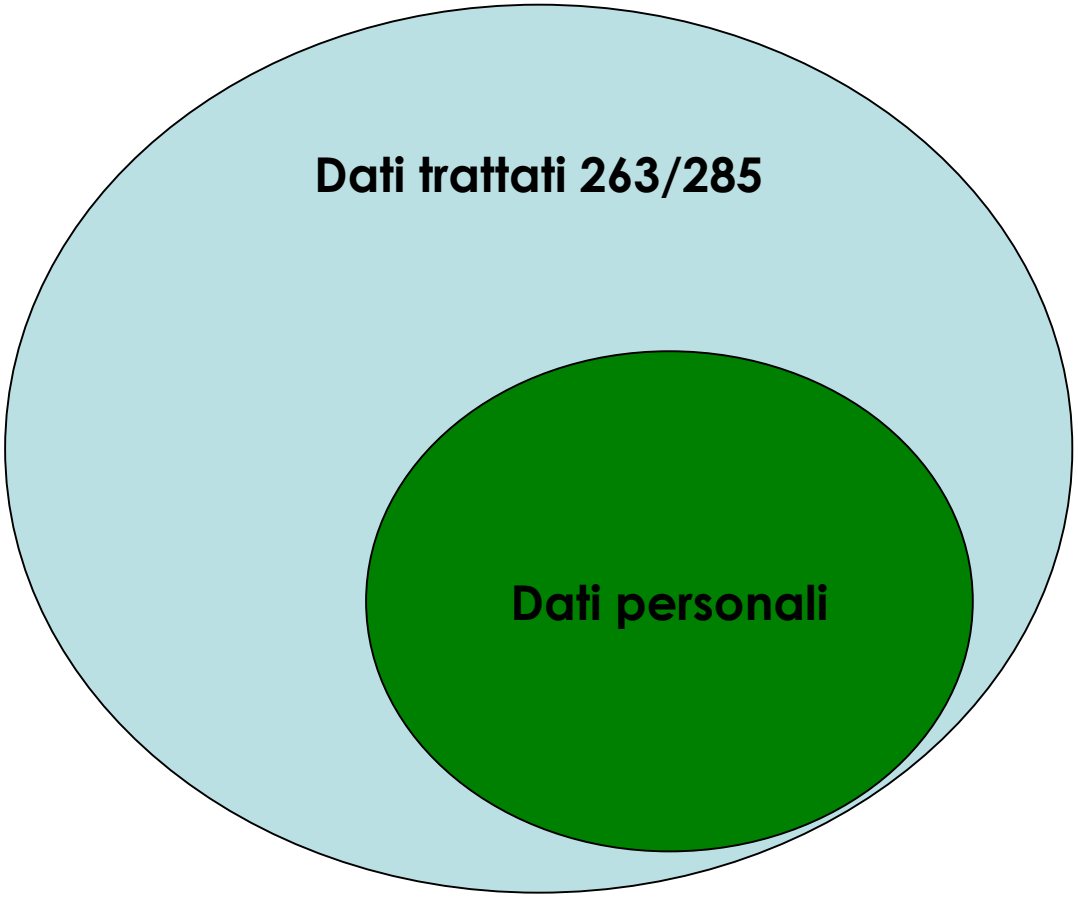
BANCO BPM

Processo esempio: Coerenza dati mutuo



BANCO BPM

263/285 e trattamento di dati personali



BANCO BPM

Attributi dei dati

PARAGRAFO NORMATIVO BI 263	ATTRIBUTO
il controllo del rischio informatico e la compliance ICT	qualità e completezza;
l'analisi del rischio informatico	riservatezza, integrità, disponibilità
la gestione della sicurezza informatica	riservatezza, integrità, disponibilità, verificabilità e accountability
il sistema di gestione dei dati	integrità, completezza e correttezza completezza, accuratezza, tempestività
	l'accountability e l'agevole verificabilità delle operazioni registrate

PARAGRAFO NORMATIVO 196/GDPR	ATTRIBUTO
Art. 11. D.Lgs 196/03 Art. 5 GDPR	•esatti e, se necessario, aggiornati; •pertinenti •completi •non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati

BANCO BPM

Attributi 263/285

TIPO	ATTRIBUTO
DATI (Qualità)	Riservatezza Integrità Disponibilità Correttezza Completezza Accuratezza Tempestività
OPERAZIONI	Accountability Verificabilità

ATTRIBUTO	DECLINAZIONE
Completezza	registrazione di tutti gli eventi, operazioni e informazioni con i pertinenti attributi necessari per le elaborazioni
Accuratezza	assenza di distorsione nei processi di registrazione, raccolta e di successivo trattamento dei dati
Tempestività	

BANCO BPM

Data quality: standard

ISO 25012 DATA QUALITY
Accuracy
Completeness
Consistency
Credibility
Currentness
Accessibility
Compliance
Confidentiality
Efficiency
Precision
Traceability
Understandability
Availability
Portability
Recoverability

TABLE II
INFORMATION QUALITY FRAMEWORK

Characteristics	Sub Characteristics	Point of View	Mapped Characteristics from [8,23,24]
Information Accuracy	Correctness	I	Correctness, Error Rate
	Credibility	I	Objectivity, Believability, Impartiality, Trustworthiness, Reliability, Reputation, Neutrality
	Currentness	I	Timeliness, Currency, Validity, Expiration, Durability
	Precision	I/S	Precision
	Traceability	I/S	Verifiability, Origin, Source, Attributability, Authority, provability.
Information Accessibility	Accessibility	I/S	Accessibility, Obtainability,
Information Appropriateness	Completeness	I	Comprehensiveness
	Understandability	I/S	Clarity, Interpretability, Reduction of complexity.
	Consistency	I	Semantic consistency
	Representational Adequacy	S	Concise Representation, Right amount, Non Duplication, Ordering, Attribute Granularity, Variability, Essentialness
	Value Added	S	Applicability, Objectivity, Utility, Helpfulness, Novelty, Beneficialness, Relevancy.
Efficiency	Efficiency	I/S	Speed, Response Time.
Confidentiality	Confidentiality	I/S	Privacy, security
Availability	Availability	S	Availability
Portability	Portability	S	Portability
Recoverability	Recoverability	S	Recoverability

Information Quality Evaluation Framework: Extending ISO 25012 Data Quality Model
Irfan Rafique, Philip Lew, Maissom Qanber Abbasi and Zhang Li
World Academy of Science, Engineering and Technology Vol:6 2012-05-24

BANCO BPM

GDPR: Principi applicabili al trattamento di dati personali

Principi applicabili al trattamento di dati personali	
"liceità, equità e trasparenza"	Liceità
	Equità
	Trasparenza
Finalità *"limitazione della finalità"*	Determinate
	Esplicite
	Legittime
Rispetto alle finalità per le quali sono trattati *"minimizzazione dei dati"*	Adeguati
	Pertinenti
	Limitati
"esattezza"	Esatti
	Aggiornati
"limitazione della conservazione"	Conservati per il tempo strettamente necessario
Adeguata sicurezza dei dati personali da *"integrità e riservatezza"*	trattamenti non autorizzati
	trattamenti illeciti
	perdita
	distruzione
	danno accidentali

BANCO BPM

Principi Dlgs 196/03 - Esattezza

Art. 11 (Modalità del trattamento e requisiti dei dati)

…

c) esatti e, se necessario, aggiornati;

…

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

La violazione dell'articolo 11 non è specificatamente sanzionata

BANCO BPM

Principi GDPR - Esattezza

Articolo 5 **Principi applicabili al trattamento di dati personali**

1. I dati personali sono:

…

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

La violazione dell'articolo 5 è punita con la massima sanzione

BANCO BPM

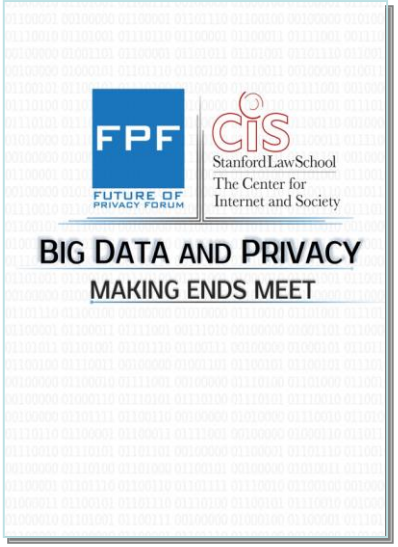
Esattezza dei dati

Big data enthusiasts have argued that companies should embrace "messy" data; that errors in databases actually help enhance knowledge discovery. In the consumer reporting context, fuzzy matching and errors have nearly wrecked individuals' lives.

One well-known anecdote concerns Judy Thomas, who sued Trans Union for regularly mixing her report with a Judith Upton.

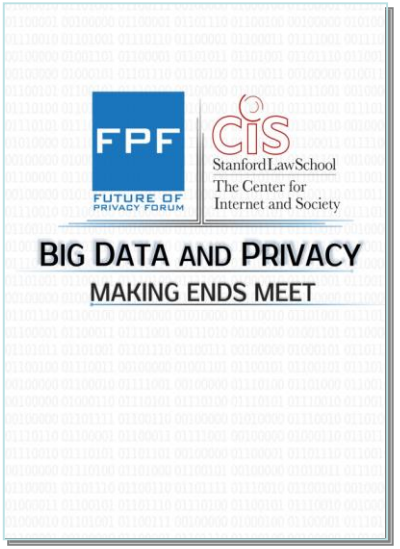
As FCRA expert Evan Hendricks explained, **"Upton's Social Security number was only one digit different than Thomas' SSN.**

That, combined with three common letters in the first name, was sufficient to cause a regular merging of the two women's credit histories."



BANCO BPM

Esattezza dei dati

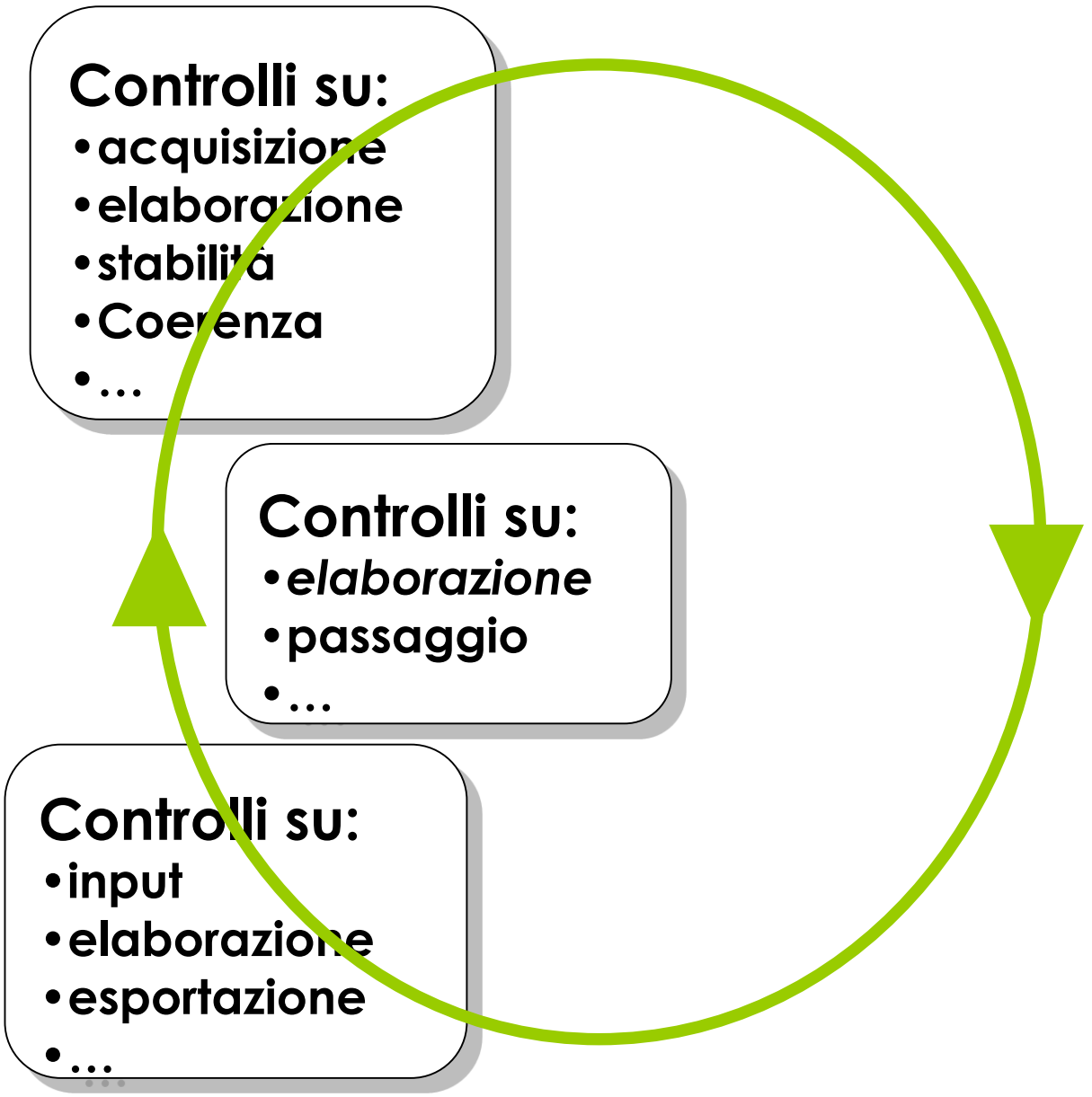


But this problem is not just anecdotal; it is structural. In a landmark and labor intensive study, academics working in conjunction with the FTC studied almost **3,000 credit reports belonging to 1,000 consumers and found that 26 percent had "material" errors—problems serious enough to affect the consumers' credit scores.**

Under the most conservative definition of error, this means that 23 million Americans have material errors on a consumer report.

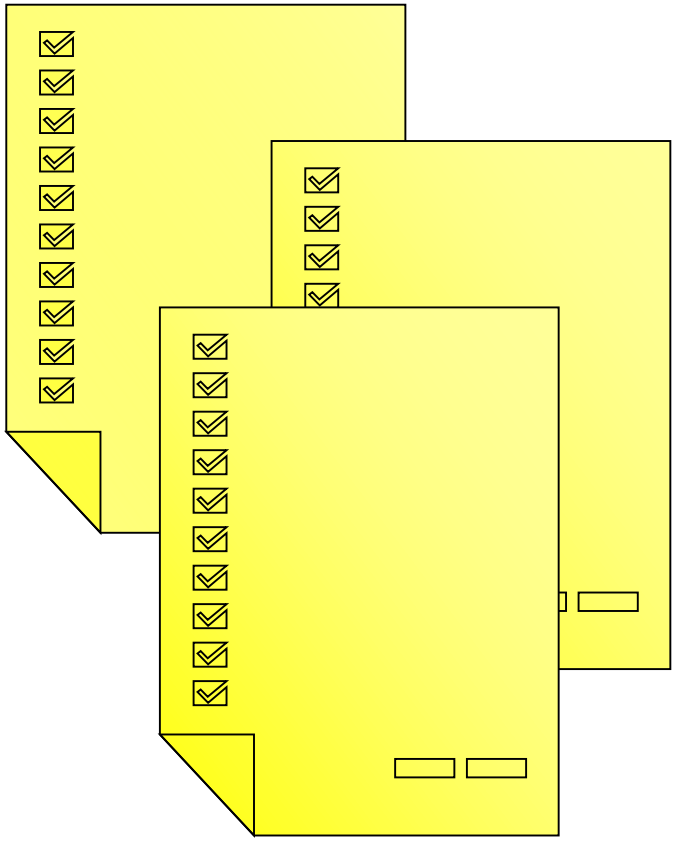
These errors matter: five percent of the study participants had errors that once corrected, improved their credit score such that they could obtain credit at a lower price.

BANCO BPM


Controlli su:
•acquisizione
•elaborazione
•stabilità
•Coerenza
•…
Controlli su:
•*elaborazione*
•passaggio
•…
Controlli su:
•input
•elaborazione
•esportazione
•…

BANCO BPM

Fonti di errore nei dati – fattori di mitigazione



INPUT MANUALE

Caricamento dati errati

ELABORAZIONE DATI

Algoritmi errati
Algoritmi incompleti
Algoritmi non correttamente implementati
Dati di partenza errati
Risultati intermedi errati
Malfunzionamenti hw/sw
Modelli di verifica

INTERAZIONE APPLICAZIONI

Estrazione dati errata
Trasferimento dati errato o mancante
Acquisizione dati errato o ripetuto

BANCO BPM

Fonti di errore nei dati – fattori di mitigazione

INPUT MANUALE

- Documentazione adeguata
- Help on line
- Formazione utenti
- Tracciatura delle operazioni eseguite (tempo, autore, dato modificato)

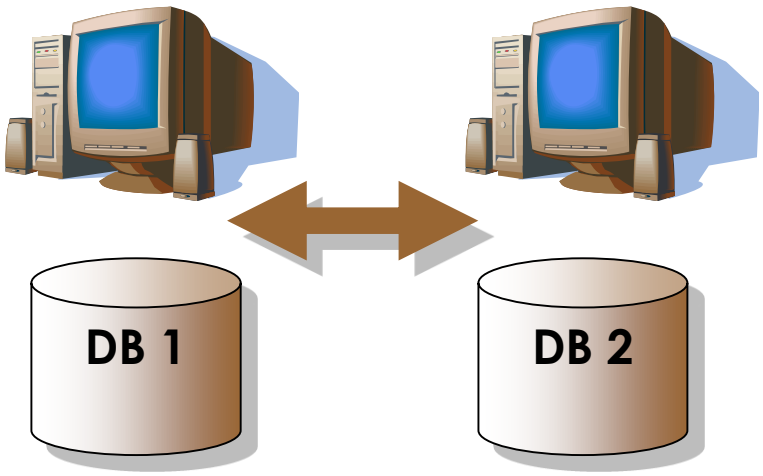
FATTORI DI MITIGAZIONE

- Validazione dati
  - tipo, lunghezza…
  - valore atteso
  - range possibile
  - scostamento rispetto al precedente
  - obbligatorietà
- Selezione da valori predefiniti
- Coerenza dei dati inseriti
- Segnalazione dei dati errati
- Rifiuto di dati incompleti
- Completezza delle maschere
- Facilità d'uso del caricamento dati
- Facilità d'uso dell'applicazione
- Standardizzazione delle videate
- Standardizzazione dei comandi

BANCO BPM

Fonti di errore nei dati – fattori di mitigazione degli errori

INTERAZIONE



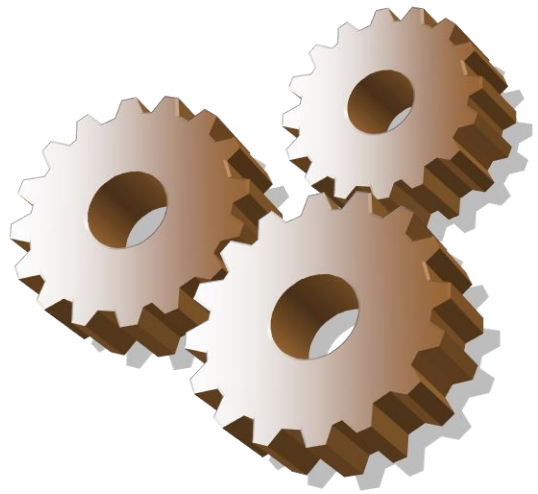
FATTORI DI MITIGAZIONE

- E' previsto un trasferimento dati (on line o batch) con altre applicazioni tale per cui non è necessario inserire lo stesso dato in applicazioni diverse
- Se il trasferimento prevede passaggi intermedi è possibile analizzare il risultato della elaborazione parziale
- E' prevista una verifica che i dati ricevuti corrispondano a quelli inoltrati
- E' previsto un meccanismo di gestione dell'errore nel trasferimento dei flussi

BANCO BPM

Fonti di errore nei dati – fattori di mitigazione

ELABORAZIONE



FATTORI DI MITIGAZIONE

- Test elaborazione su casi noti
- Documentazione test
- Certificazione da parte del produttore
- Tracciatura dei dati intermedi di elaborazione
- Monitoraggio dei risultati
- Segnalazione di anomalie
- Separazione degli ambienti di sviluppo, test e produzione
- Le applicazioni ed i database sono adeguatamente documentati
- Sono disponibili modelli per la verifica della stabilità e della coerenza dei dati

BANCO BPM

Fonti di errore nei dati – fattori di mitigazione

MATURITA

FATTORI DI MITIGAZIONE

- Il caricamento dei dati nelle tabelle avviene da parte dell'utente
- Non sono presenti dati caricati direttamene nel codice
- L'applicazione ed il sottostante database sono adeguatamente documentati
- L'applicazione è parametrica ed è personalizzabile senza intervenire sul codice
- Le competenze per la manutenzione dell'applicazione sono interne e sono diffuse
- Le applicazioni sono complete di tutte le funzionalità richieste
- Il livello di automazione è elevato
- Le applicazioni interagiscono fra loro

BANCO BPM

Rilevazione di possibili errori nei dati

Fonti riconducibili direttamente ai sistemi informativi, tra le quali:

- **Segnalazioni di malfunzionamenti da parte di utenti sia interni che esterni**
- **Richieste di intervento da parte degli utenti per risolvere situazioni anomale (errori nelle applicazioni e nei sistemi, degrado delle prestazioni, perdite o alterazioni di dati, rotture…)**
- **Log**
- **Righe di codice modificate**
- **Database incidenti**
- **Rapporti di intervento**

Il processo si raccorda con il monitoraggio di sistemi, accessi e operazioni (cfr. par. 3) nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi da parte degli utenti interni ed esterni, favorendo l'assunzione di iniziative di prevenzione.

BANCO BPM

Gestione anomalie – processo di gestione

Fonti connesse in modo indiretto ai problemi generati dai sistemi informativi, quali:

- **Reclami dei clienti (rate del mutuo errate, condizioni riportate negli estratti conto non in linea con quelle contrattualizzate…)**
- **Reclami dei fornitori (ad esempio, ritardi nei pagamenti)**
- **Rilievi dell'audit**
- **Rilievi della Vigilanza**

☑ Esiste una procedura formalizzata per la gestione dei reclami?

☑ I reclami sono centralizzati indipendentemente dal canale utilizzato dal cliente (filiale, lettera, e-mail…)?

☑ Esiste un processo di analisi per collezionare eventi simili che possano ricondurre sia ad un malfunzionamento del sistema informativo (ad esempio errata rata di un mutuo)?

☑ Esiste un processo di comunicazione con chi gestisce i sistemi informativi?

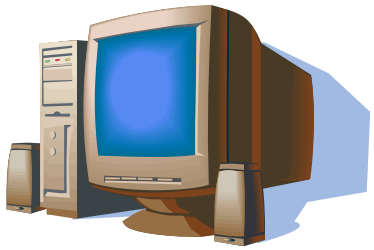
☑ I reclami sono adeguatamente classificati?

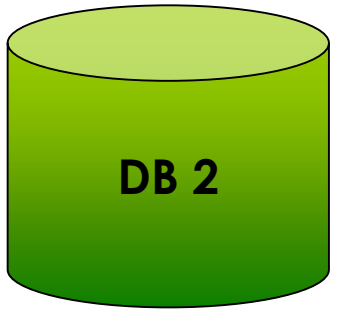
BANCO BPM

LA QUALITA' DEI DATI E' INFLUENZATA DA:

- Variazione delle applicazioni in seguito a:
  - Nuove release software
  - Nuovi prodotti/servizi
  - Variazioni normative
- Variazione dei sistemi informativi
  - Hardware
  - Software di base
  - Middelware
- Variazione dei processi aziendali

- Malfunzionamenti dei sistemi
- Competenza degli utenti
- Competenza dell'IT
- ….

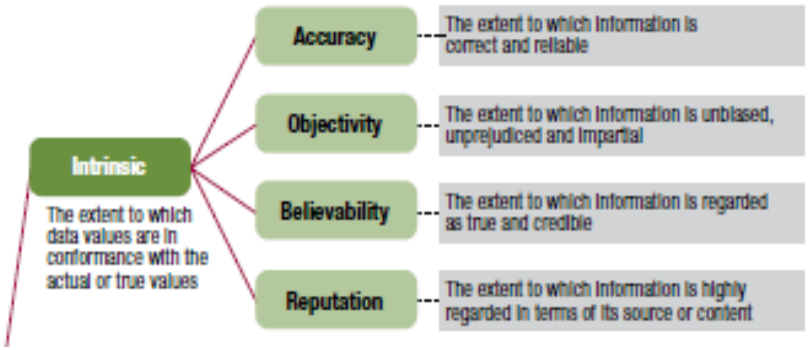


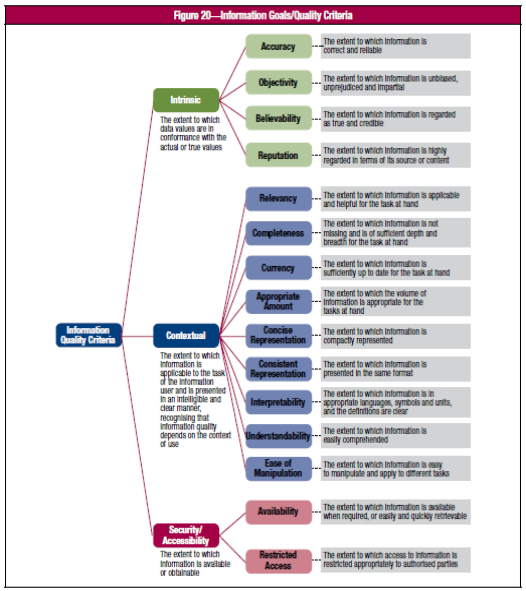


BANCO BPM

Data quality: strumenti

COBIT 5 Enabling information





BANCO BPM

Data quality: indicatori

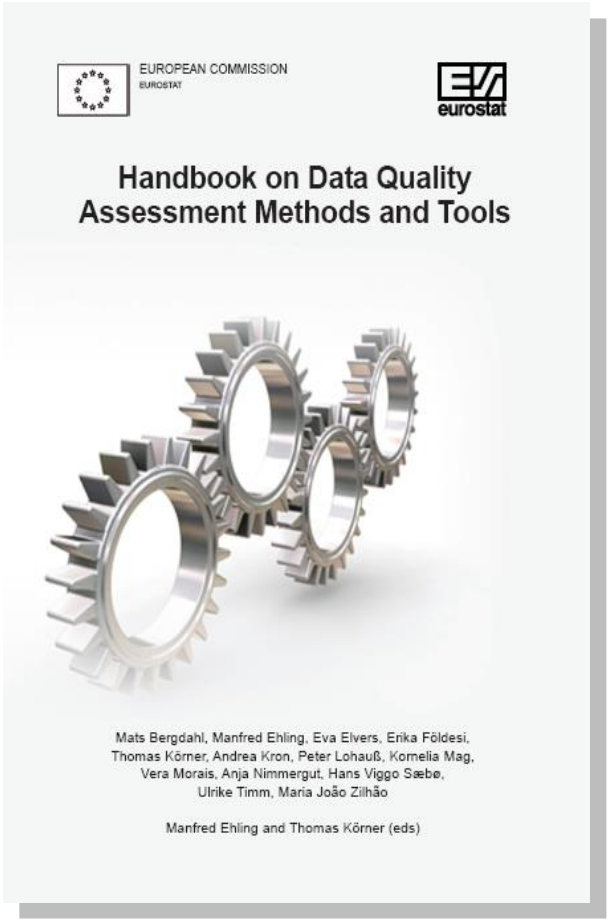
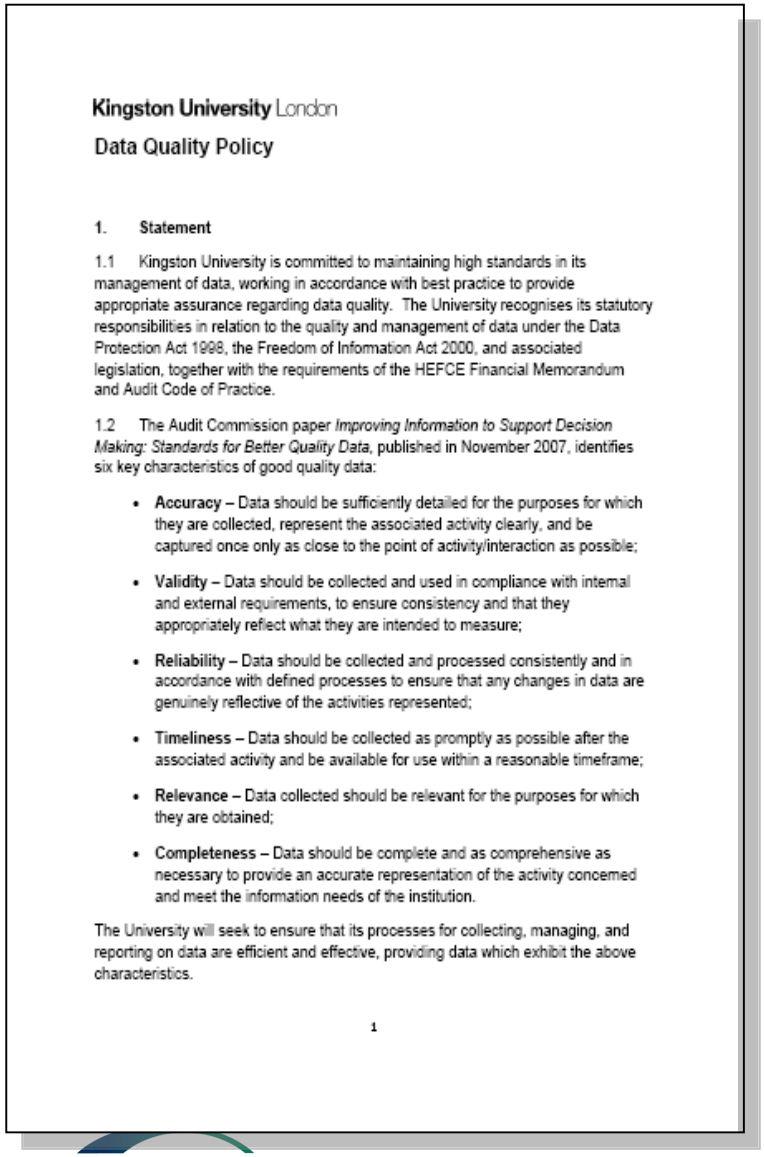


Table 1: List of Standard Quality Indicators (Eurostat 2005d)

Quality component	Indicator		1=Key 2=Supportive 3=Advanced
Relevance	R1.	User satisfaction index	3
	R2.	Rate of available statistics	1
Accuracy	A1.	Coefficient of variation	1
	A2.	Unit response rate (un-weighted/weighted)	2
	A3.	Item response rate (un-weighted/weighted)	2
	A4.	Imputation rate and ratio	2
	A5.	Over-coverage and misclassification rates	2
	A6.	Geographical under-coverage ratio	1
	A7.	Average size of revisions	1
Timeliness and Punctuality	T1.	Punctuality of time schedule of effective publication	1
	T2.	Time lag between the end of reference period and the date of first results	1
	T3.	Time lag between the end of reference period and the date of the final results	1
Accessibility and Clarity	AC1.	Number of publications disseminated and/ or sold	1
	AC2.	Number of accesses to databases	1
	AC3.	Rate of completeness of metadata information for released statistics.	3
Comparability	C1.	Length of comparable time-series	1
	C2.	Number of comparable time-series	1
	C3.	Rate of differences in concepts and measurement from European norms	3
	C4.	Asymmetries for statistics mirror flows	1
Coherence	CH1.	Rate of statistics that satisfies the requirements for the main secondary use	3

BANCO BPM

Data quality: policy



Kingston University London

Data Quality Policy

1. Statement

1.1 Kingston University is committed to maintaining high standards in its management of data, working in accordance with best practice to provide appropriate assurance regarding data quality. The University recognises its statutory responsibilities in relation to the quality and management of data under the Data Protection Act 1998, the Freedom of Information Act 2000, and associated legislation, together with the requirements of the HEFCE Financial Memorandum and Audit Code of Practice.

1.2 The Audit Commission paper *Improving Information to Support Decision Making: Standards for Better Quality Data*, published in November 2007, identifies six key characteristics of good quality data:

- **Accuracy** – Data should be sufficiently detailed for the purposes for which they are collected, represent the associated activity clearly, and be captured once only as close to the point of activity/interaction as possible;
- **Validity** – Data should be collected and used in compliance with internal and external requirements, to ensure consistency and that they appropriately reflect what they are intended to measure;
- **Reliability** – Data should be collected and processed consistently and in accordance with defined processes to ensure that any changes in data are genuinely reflective of the activities represented;
- **Timeliness** – Data should be collected as promptly as possible after the associated activity and be available for use within a reasonable timeframe;
- **Relevance** – Data collected should be relevant for the purposes for which they are obtained;
- **Completeness** – Data should be complete and as comprehensive as necessary to provide an accurate representation of the activity concerned and meet the information needs of the institution.

The University will seek to ensure that its processes for collecting, managing, and reporting on data are efficient and effective, providing data which exhibit the above characteristics.

1

1. Statement
2. Scope
3. Objectives
3.1 Appropriate Awareness and Responsibility
3.2 Appropriate Procedures
3.3 Appropriate Systems and Processes
4. Governance and Accountability
4.1 Audit Committee

BANCO BPM

Sicurezza

BANCO BPM

Sicurezza 196 e Sicurezza GDPR

Art. 31. **Obblighi di sicurezza (196/03)**

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, **dei dati stessi**, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32 **Sicurezza del trattamento (GDPR)**

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche**, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

BANCO BPM

Variazione del perimetro di tutela

1996

Dir. 45/96 CE: "le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata" *(cons. 10)*

2014

WP29, op. 218/14: "7/ Risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria (…).

8/ In the context referred to above, the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy **but may also involve other fundamental rights** such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

2016

GDPR Art. 1.2 Il presente regolamento **protegge i diritti e le libertà fondamentali delle persone fisiche**, in particolare il **diritto alla protezione dei dati personali**.

BANCO BPM

I diritti e le libertà fondamentali

(75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da **trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;** se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

BANCO BPM

Diritti e libertà delle persone fisiche

Diritti e libertà delle persone fisiche
danno fisico
danno materiale
danno morale
discriminazioni
furto o usurpazione d'identità
perdite finanziarie
pregiudizio alla reputazione
perdita di riservatezza dei dati protetti da segreto professionale
decifratura non autorizzata della pseudonimizzazione
danno economico o sociale significativo

BANCO BPM

PIA e Sicurezza

Articolo 35 **Valutazione d'impatto sulla protezione dei dati**

1.Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Articolo 32 **Sicurezza del trattamento**

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del **rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche**, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

BANCO BPM


PIA
Violazione di dati personali
Diritti e libertà fondamentali delle persone fisiche
Sicurezza del trattamento

BANCO BPM

D.Lgs 196/03 Sicurezza

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono **custoditi e controllati**, anche in relazione alle **conoscenze acquisite in base al progresso tecnico**, alla **natura dei dati** e alle **specifiche caratteristiche del trattamento**, in modo da **ridurre al minimo**, mediante l'adozione di **idonee e preventive misure di sicurezza**, i rischi di **distruzione o perdita**, anche **accidentale**, dei dati stessi, di **accesso non autorizzato** o di **trattamento non consentito** o **non conforme alle finalità della raccolta**.

BANCO BPM

GDPR: Sicurezza

Articolo 32 **Sicurezza del trattamento**

1.Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura, dell'oggetto, del contesto e delle finalità del trattamento**, come anche del **rischio** di varia **probabilità e gravità** per i **diritti e le libertà delle persone fisiche**, il titolare del trattamento e il responsabile del trattamento mettono in atto **misure tecniche e organizzative ADEGUATE** per garantire un **livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, se del caso:

a) la **PSEUDONIMIZZAZIONE** e la **CIFRATURA** dei dati personali;

b) la capacità di assicurare su base permanente la **riservatezza, l'integrità, la disponibilità** e la **resilienza** dei **sistemi** e dei **servizi** di trattamento;

c) la capacità di **ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di **incidente fisico o tecnico**;

d) una procedura per **testare, verificare** e **valutare regolarmente** l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

BANCO BPM

GDPR: Sicurezza

2.Nel valutare l'**ADEGUATO LIVELLO DI SICUREZZA**, si tiene conto in special modo dei **rischi** presentati dal trattamento che derivano in particolare dalla **distruzione**, **dalla perdita**, **dalla modifica**, **dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale**, a dati personali trasmessi, conservati o comunque trattati.

3.L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4.Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

BANCO BPM

GDPR: Sicurezza

Articolo 5 **Principi applicabili al trattamento di dati personali**

1.I dati personali sono:

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

BANCO BPM

Valutazione dell'adeguato livello di sicurezza

GDPR: Valutazione dell'adeguato livello di sicurezza		
rischi presentati da trattamenti di dati derivanti in particolare	distruzione	in modo accidentale o illegale
	perdita	
	modifica	
	divulgazione non autorizzata	

BANCO BPM

285: La sicurezza informatica

La funzione di sicurezza informatica è deputata allo svolgimento dei compiti specialistici in materia di sicurezza delle risorse ICT. In particolare:

— segue la redazione e l'aggiornamento delle *policy* di sicurezza e delle istruzioni operative;

— assicura la coerenza dei presidi di sicurezza con le *policy* approvate;

— partecipa alla progettazione, realizzazione e manutenzione dei presidi di sicurezza dei *data center*;

— partecipa alla valutazione del rischio potenziale nonché all'individuazione dei presidi di sicurezza nell'ambito del processo di analisi del rischio informatico (cfr. Sezione III);

— assicura il monitoraggio nel continuo delle minacce applicabili alle diverse risorse informatiche (cfr. Sezione IV, par. 3);

— segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un sistema nuovo o modificato (cfr. Sezione IV, par. 5).

Nelle realtà più complesse, l'indipendenza di giudizio rispetto alle funzioni operative è assicurata da un'adeguata collocazione organizzativa.

BANCO BPM

285: La gestione della sicurezza informatica

1. Premessa

La gestione della sicurezza informatica comprende i processi e le misure volti, in raccordo con la generale azione aziendale per preservare la sicurezza delle informazioni e dei beni aziendali, a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability*, appropriata e coerente lungo l'intero ciclo di vita.

Obiettivo di tale processo è anche di contribuire alla conformità del sistema informativo alle norme di legge e a regolamenti interni ed esterni.

La struttura dei processi e l'intensità dei presidi da porre in atto dipende dalle risultanze del processo di analisi dei rischi (cfr. Sezione III).

BANCO BPM

285: Policy di sicurezza

La *policy* di sicurezza informatica è approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale e alle terze parti coinvolte nella gestione di informazioni e componenti del sistema informativo. Essa riporta:

— gli obiettivi del processo di gestione della sicurezza informatica in linea con la propensione al rischio informatico definito a livello aziendale (cfr. Sezione II, par. 2); tali obiettivi sono espressi in termini di esigenze di protezione e di controllo del rischio tecnologico;

— i principi generali di sicurezza sull'utilizzo e la gestione del sistema informativo da parte dei diversi profili aziendali;

— i ruoli e le responsabilità connessi alla funzione di sicurezza informatica nonché all'aggiornamento e verifica delle *policy*;

— il quadro di riferimento organizzativo e metodologico dei processi di gestione dell'ICT deputati a garantire l'appropriato livello di protezione;

— le linee di indirizzo per le attività di comunicazione, formazione e sensibilizzazione delle diverse classi di utenti;

— un richiamo alle norme interne che disciplinano le conseguenze di violazioni rilevate della *policy* da parte del personale;

— un richiamo alle norme di legge e alle altre normative esterne applicabili inerenti alla sicurezza di informazioni e risorse ICT, incluse le norme riportate nella presente Sezione.

La *policy* di sicurezza può fare riferimento a documenti di maggiore dettaglio, ad es. linee guida o manuali operativi in tema di configurazioni e procedure di sicurezza per particolari componenti e applicazioni; *policy* dedicata per i servizi di pagamento via internet; norme per il corretto utilizzo di applicazioni aziendali trasversali, quali la posta elettronica e la navigazione internet.

La regolare revisione della *policy* di sicurezza tiene conto dell'evoluzione del campo di attività, dei prodotti forniti, delle tecnologie e dei rischi fronteggiati dall'intermediario (cfr. Sezione III).

BANCO BPM

285: La sicurezza delle informazioni e delle risorse ICT

La sicurezza delle informazioni e delle risorse informatiche è garantita attraverso misure di protezione a livello fisico e logico, la cui intensità di applicazione è graduata in relazione alle risultanze della valutazione del rischio (classificazione delle risorse informatiche in termini di sicurezza). Tali misure sono distribuite su diversi strati, così che un'eventuale falla in una linea di difesa sia coperta dalla successiva ("difesa in profondità"), comprendendo:

— i presidi fisici di difesa e le procedure di autorizzazione e controllo per l'accesso fisico a sistemi e dati (ad es., barriere perimetrali con punti di ingresso vigilati, locali ad accesso controllato con registrazione degli ingressi e delle uscite);

— la regolamentazione dell'accesso logico a reti, sistemi, basi di dati sulla base delle effettive esigenze operative (principio del *need to know)*; i diritti di accesso sono accordati, mediante ricorso ad opportuni profili abilitativi, previa formale autorizzazione; l'elenco degli utenti abilitati è sottoposto a verifica con periodicità definita;

— la procedura di autenticazione per l'accesso alle applicazioni e ai sistemi; in particolare sono garantiti l'univoca associazione a ciascun utente delle proprie credenziali di accesso, il presidio della riservatezza dei fattori di autenticazione (1), l'osservanza degli standard definiti all'interno nonché delle normative applicabili, ad es. in materia di composizione e gestione della password, di limiti ai tentativi di accesso, di lunghezza di chiavi crittografiche;

— la segmentazione della rete di telecomunicazione, con controllo dei flussi scambiati, in particolare tra domini connotati da diversi livelli di sicurezza (ad es., sistemi e utenti interni, applicazioni *core,* sistemi e utenti esterni); l'accesso a sistemi e servizi critici tramite canali pubblici (ad es., nel caso dell'*e-banking* tramite internet) sono presidiati in modo da soddisfare rigorosi requisiti di sicurezza e fornire un livello di protezione conforme ai rischi da fronteggiare; con riferimento ai servizi di pagamento tramite internet si applicano gli "Orientamenti finali in materia di sicurezza dei pagamenti via internet" emanati dall'ABE, secondo quanto specificato nella Sezione VII;

BANCO BPM

285: La sicurezza delle informazioni e delle risorse ICT

— l'adozione di metodologie e tecniche per lo sviluppo sicuro del software quale possibile presidio di difesa per componenti valutate nell'analisi del rischio informatico a un livello di rischio potenziale elevato;

— la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software tra di essi (par. 5), al fine di evitare – di norma – l'accesso a dati riservati e componenti critiche da parte del personale addetto allo sviluppo (2); l'ambiente di produzione è sottoposto a misure più restrittive di controllo degli accessi e delle modifiche;

— i criteri per la selezione e la gestione del personale adibito al trattamento dei dati e allo svolgimento di operazioni critiche (amministratori di sistema e utenti privilegiati) con particolare riguardo alla valutazione delle competenze e dell'affidabilità del personale, alla stipula di specifici impegni di riservatezza nonché alla gestione nel continuo delle mansioni assegnate (ad es., per mezzo di verifiche periodiche degli elenchi del personale abilitato e di misure di *job rotation*);

— le procedure per lo svolgimento delle operazioni critiche, garantendo il rispetto dei principi del minimo privilegio e della segregazione dei compiti (ad es., specifiche procedure di abilitazione e di autenticazione, controlli di tipo *four eyes* (3), o di verifica giornaliera *ex post*);

— il monitoraggio, anche attraverso l'analisi di log e tracce di *audit*, di accessi, operazioni e altri eventi al fine di prevenire e gestire gli incidenti di sicurezza informatica; le attività degli amministratori di sistema e altri utenti privilegiati delle componenti critiche sono sottoposte a stretto controllo;

— il monitoraggio continuativo delle minacce e delle vulnerabilità di sicurezza;

— le regole di tracciabilità delle azioni svolte, finalizzate a consentire la verifica a posteriori delle operazioni critiche, con l'archiviazione dell'autore, data e ora (4), contesto operativo e altre caratteristiche salienti della transazione. Le tracce elettroniche sono conservate per un periodo non inferiore a 24 mesi in archivi non modificabili o le cui modifiche sono puntualmente registrate.

BANCO BPM

285: La gestione degli incidenti di sicurezza informatica

La gestione degli incidenti di sicurezza informatica segue procedure formalmente definite, con l'obiettivo di minimizzare l'impatto di eventi avversi e garantire il tempestivo ripristino del regolare funzionamento dei servizi e delle risorse ICT coinvolti. Le funzioni a cui comunicare l'incidente sono individuate secondo un'opportuna procedura di *escalation*; i casi più gravi che comportino rischi di interruzione della continuità operativa sono segnalati alla struttura preposta a dichiarare lo stato di crisi (cfr. Capitolo 5).

A seguito dell'analisi degli incidenti di sicurezza informatica e dei relativi rilievi delle funzioni di *audit* e della *compliance* sono definite e monitorate le azioni correttive.

In ogni caso, le informazioni salienti dell'evento e i passi seguiti nella gestione dello stesso sono documentati.

Il processo si raccorda con il monitoraggio di sistemi, accessi e operazioni (cfr. par. 3) nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi da parte degli utenti interni ed esterni, favorendo l'assunzione di iniziative di prevenzione (8).

Le procedure definite per gravi incidenti di sicurezza informatica includono la cooperazione con le forze dell'ordine preposte e con gli altri operatori o enti coinvolti, anche in caso di fuoriuscite di informazioni.

I gravi incidenti di sicurezza informatica sono comunicati tempestivamente alla Banca centrale europea o alla Banca d'Italia, con l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela nonché i seguenti dati, accertati o presunti: i) data e ora dell'accadimento o della manifestazione dell'incidente; ii) risorse e servizi coinvolti; iii) cause, tempi e modalità previsti per il pieno ripristino dei livelli di disponibilità e sicurezza definiti e per il completo accertamento dei fatti connessi; iv) descrizione delle azioni intraprese e dei risultati ottenuti; v) una valutazione dei danni delle perdite economiche o danni d'immagine.

BANCO BPM

Sicurezza: GDPR e 285

BANCO BPM

Sicurezza: violazione di dati personali

BANCO BPM

GDPR

Articolo 33 **Notifica di una violazione dei dati personali all'autorità di controllo**

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.

Articolo 4 **Definizioni** Ai fini del presente regolamento s'intende per:

…

12) **«violazione dei dati personali»:**la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

BANCO BPM

Altre normative che prevedono la notifica

PSD2

Articolo 96

Notifica degli incidenti

1. In caso di grave incidente operativo o relativo alla sicurezza, i prestatori di servizi
pagamento lo notificano senza indugio all'autorità competente dello Stato memb
del prestatore di servizi di pagamento

gli interessi finanziari dei propri utenti di
to informa senza indugio i propri ute
a disposizione che possono adotta

eIDAS

Articolo 19

Requisiti di sicurezza relativi ai prestatori di servizi fiduciari

1. I prestatori di servizi fiduciari qualificati e non qualificati adott
organizzative appropriate per gestire i rischi legati alla sicurezz
prestati. Tenuto conto degli ultimi sviluppi tecnologici, tali mis
sicurezza commisurato al grado di rischio esistente. In partico
prevenire e minimizzare l'impatto degli incidenti di sicurezza e
degli effetti negat
2. Senza indug
servizi fiduciar
applicabile
delle inform
perdite di i
personali iv
Qualora sia
negativi su
di servizi fi
sicurezza d
Ove appro
riguardi du
vigilanza n
L'organism
di farlo, ov
integrità si
3. L'organ
violazione
4. La Com

Circolare 285

l'autorità competente dello St
dell'incidente all'ABE e alla BC

6. La gestione degli incidenti di sicurezza informatica

La gestione degli incidenti di sicurezza informatica segue procedure f
l'obiettivo di minimizzare l'impatto di eventi avversi e garantire il temp
regolare funzionamento dei servizi e delle risorse ICT coinvolti. Le funzi
a procedura di esc
operativa sono s
matica e dei relat
le azioni correttiv
assi seguiti nella g
accessi e operaz
azioni di problemi
di prevenzione (9
informatica inclu
tori o enti coinvol
cati tempestivam
orto sintetico reca
erni e alla clientel
o della manifesta

Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie 12 maggio 2011

2) Misure opportune:

…

h) Comunicazioni al Garante (punto 5.2).

Le banche comunicano tempestivamente al Garante i casi in cui risulti accertata una violazione, accidentale o illecita, nella protezione dei dati personali, di particolare rilevanza.

Circolare 285

I **gravi incidenti di sicurezza informatica sono comunicati tempestivamente alla Banca centrale europea o alla Banca d'Italia**, con l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela nonché i seguenti dati, accertati o presunti: i) data e ora dell'accadimento o della manifestazione dell'incidente; ii) risorse e servizi coinvolti; iii) cause, tempi e modalità previsti per il pieno ripristino dei livelli di disponibilità e sicurezza definiti e per il completo accertamento dei fatti connessi; iv) descrizione delle azioni intraprese e dei risultati ottenuti; v) una valutazione dei danni delle perdite economiche o danni d'immagine.

"*incidente di sicurezza informatica*": ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es., frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi);

— "*grave incidente di sicurezza informatica*": un incidente di sicurezza informatica da cui derivi almeno una delle seguenti conseguenze:

a. perdite economiche elevate o prolungati disservizi per l'intermediario, anche a seguito di ripetuti incidenti di minore entità;

b. disservizi rilevanti sulla clientela e altri soggetti (ad es., intermediari o infrastrutture di pagamento); la valutazione della gravità considera il numero dei clienti o controparti potenzialmente coinvolti e l'ammontare a rischio;

c. il rischio di inficiare la capacità della banca di conformarsi alle condizioni e agli obblighi di legge o previsti dalla disciplina di vigilanza;

BANCO BPM

È diverso il livello per il quale è necessario procedere alla notifica

Circolare 285

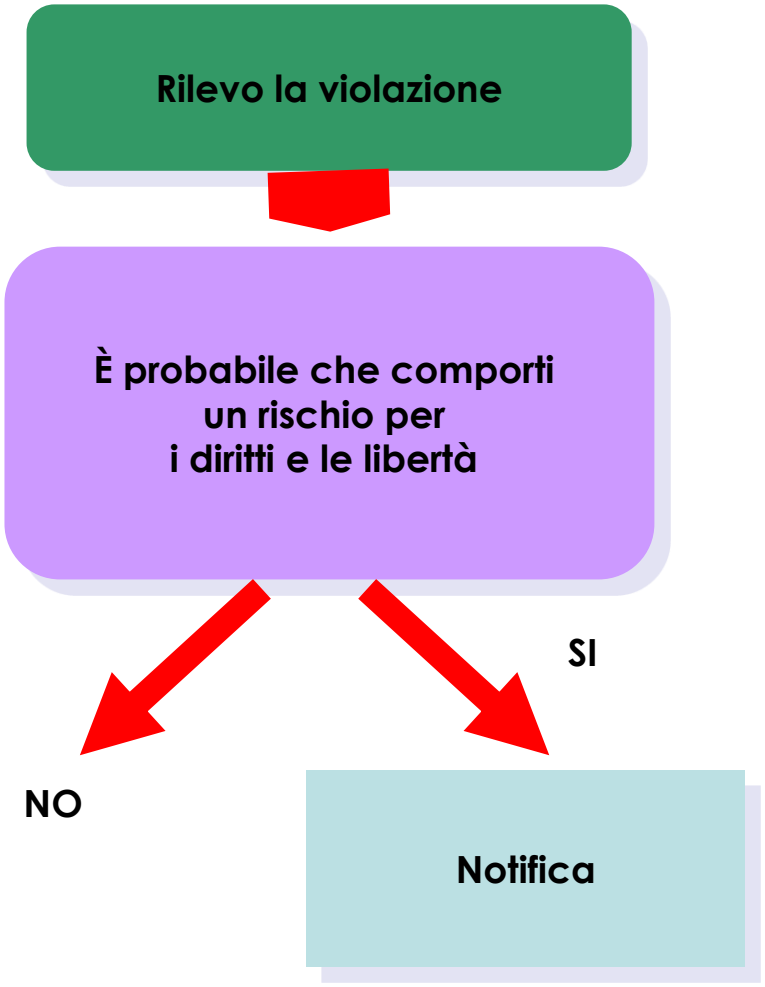
*I **GRAVI INCIDENTI** di sicurezza informatica sono comunicati tempestivamente alla Banca centrale europea o alla Banca d'Italia*

GDPR

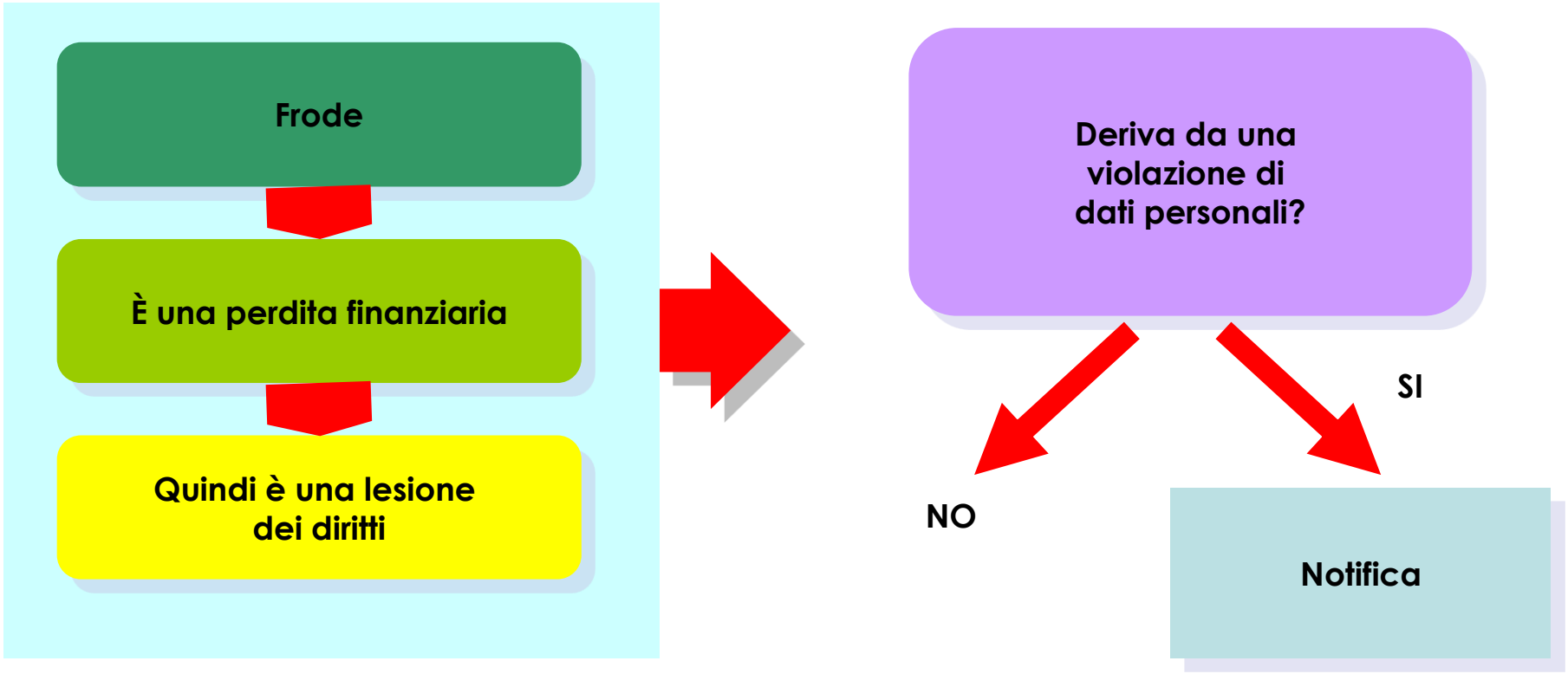
*In caso di **VIOLAZIONE DEI DATI PERSONALI**, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, **a meno che sia improbabile che la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

BANCO BPM

Rilevo una violazione



Rilevo un effetto che può derivare da violazione



BANCO BPM

Quando è necessario notificare nel caso del GDPR?

Sempre

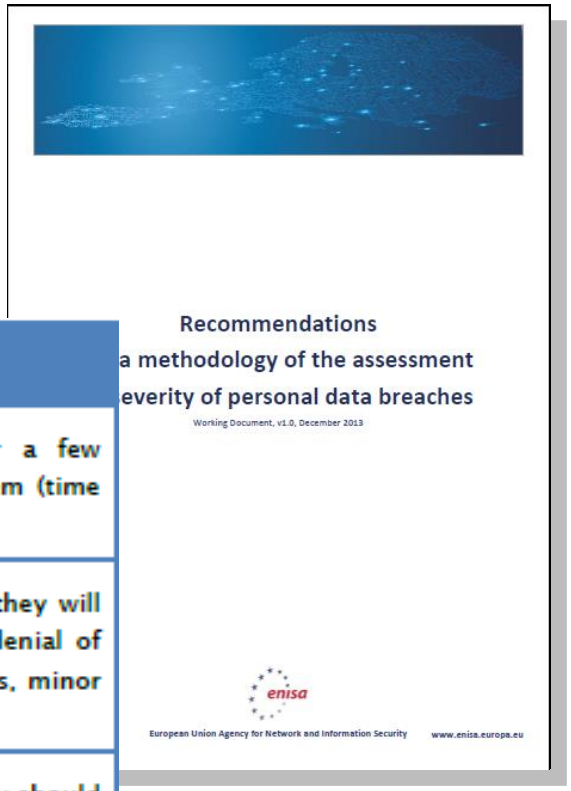
a meno che sia **improbabile** che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Diritti e le libertà delle persone fisiche
danno fisico
danno materiale
danno morale
discriminazioni
furto o usurpazione d'identità
perdite finanziarie
pregiudizio alla reputazione
perdita di riservatezza dei dati protetti da segreto professionale
decifratura non autorizzata della pseudonimizzazione
danno economico o sociale significativo

BANCO BPM

Strumenti di valutazione

Ci sono strumenti che consentono
di dare un peso alla violazione?



Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with funds, blacklisting by banks, subpoena, worsening of health,
4 ≤ SE	Very High	Individuals may encounter consequences, which they may substantial debt or inability physical ailments, death, etc.).

Type of personal data
Criticality of the processing operation
Volume of the personal data processed
Special characteristics of the data controller/processor
Special characteristics of the data subjects

Strumenti di valutazione

Case 1: the data come from a bank and include only a letter, through which the individual is identified as a client without providing any information about the specific relations between the client and the bank (e.g. only his/her name and address but no account number or information about transactions).
Score = 1 (by nature of the data set).

Case 2: the data come from a bank and include only a transactions history of one day without further details (e.g. account number, name and transaction).
Score = 2 (by nature of data, info that can lead to limited information about financial behaviour).

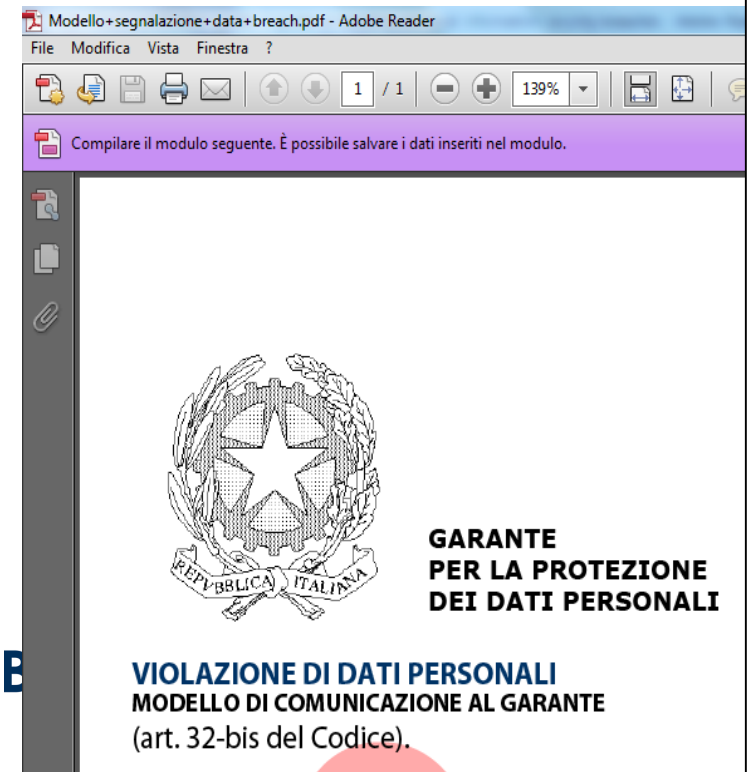
Case 3: the data come from a bank and concern account balances of clients of the last month.
Score = 3 (no alteration due to contextual factors).

Case 4: the data come from a bank and include account balances of clients of the last year, showing all transactions and related with them details.
Score = 4 (by volume and nature of data leading to profiling)

BANCO BPM

Strumenti

Ci sono buone pratiche per la effettuare la notificazione?



Allegato B al Provvedimento del 4 giugno 2015 "Linee guida in materia di dossier sanitario"

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal Provvedimento del 4 giugno 2015 *"Linee guida in materia di dossier sanitario"*, i titolari di trattamento dei dati personali effettuati mediante il *dossier* sanitario sono tenuti a comunicare al Garante all'indirizzo: databreach.dossier@pec.gpdp.it le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle proprie strutture (*cfr. punto 7.1. delle predette Linee guida*).

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Titolare del trattamento del *dossier* sanitario

Denominazione o ragione sociale _____

Provincia _____ Comune _____

Cap _____ Indirizzo _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Strumenti

Modello Garante

- Lettura (presumibilmente i dati non sono stati copiati)
- Copia (i dati sono ancora presenti sui sistemi del titolare)
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- Altro:

GDPR

- Accesso ai dati personali
- Divulgazione non autorizzata
- Modifica
- Distruzione
- Perdita

BANCO BPM

Strumenti

MAINTAIN INFORMATION SECURITY—APP 11

Protect information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

To comply with their obligations under the APPs, **agencies and organisations** should consider:

- the sensitivity of the personal information
- the harm likely to flow from a security breach
- developing a compliance and monitoring plan, and
- regularly reviewing their information security measures.

DATA BREACH OCCURS

Personal information is lost or subjected to unauthorised access, modification, use or disclosure, or other misuse or interference.

KEY STEPS IN RESPONDING TO A DATA BREACH

STEP 1	**Contain the breach and make a preliminary assessment**	• Take immediate steps to contain breach • Designate person/team to coordinate response
STEP 2	**Evaluate the risks for individuals associated with the breach**	• Consider what personal information is involved • Determine whether the context of the information is important • Establish the cause and extent of the breach • Identify what is the risk of harm
STEP 3	**Consider breach notification**	• Risk analysis on a case-by-case basis • Not all breaches necessarily warrant notification

SHOULD AFFECTED INDIVIDUALS BE NOTIFIED?

Where there is a **real risk of serious harm**, notification may enable individuals to take steps to avoid or mitigate harm. Consider:

- **Legal/contractual obligations to notify**
- Risk of harm to individuals (identity crime, physical harm, humiliation, damage to reputation, loss of business or employment opportunities

Process of Notification

- **When?** - as soon as possible
- **How?** - direct contact preferred (mail/phone)
- **Who?** - entity with the direct relationship with the affected individual
- **What?** - description of breach, type of personal information involved, steps to help mitigate, contact details for information and assistance.

SHOULD OTHERS BE NOTIFIED?

- **Office of the Australian Information Commissioner**
- Police/Law Enforcement
- Professional or Regulatory Bodies
- Other agencies or organisations affected by the breach or contractually required to notify

STEP 4	**Review the incident and take action to prevent future breaches**	• Fully investigate the cause of the breach • Consider developing a prevention plan • Option of audit to ensure plan implemented • Update security/ response plan • Make appropriate changes to policies and procedures • Revise staff training practices

Strumenti

enisa European Union Agency for Network and Information Security

MENU

Navigation menu

Personal data breach notification tool

Published under Personal data breaches
Tagged with Data protection,Data breaches,Personal Data

ENISA, in co-operation with the Office of the Federal Commissioner for Data Protection and Freedom of Information of Germany (German DPA), developed a tool for the notification of personal data breaches.

In particular, the purpose of the tool is to provide for the online completion and submission of a personal data breach notification by the data controller to the competent authority (DPA/NRA). It covers all types of personal data breaches and all types of business sectors, public or private.

Based on the input of the notification, the tool also provides to the competent authority an assessment of the severity of the breach. The assessment is based on the relevant Personal Data Breach Severity Assessment Methodology developed by ENISA in co-operation with the DPAs of Greece and Germany.

The tool is free for use by any interested party, in particular national competent authorities who would like to facilitate the notification of personal data breaches by data controllers in their countries.

If you would like to test the use of the tool and/or get a copy of the software, please send an email to the following address: isdp at enisa dot europa dot eu.

Recommended publications

Recommendations for a methodology of the assessment of...

The European Union Agency for Network and Information Security (ENISA) reviewed the existing measures and the procedures in EU Member States with...

Published on December 20, 2013

References

- Federal Commissioner for Data Protection and Freedom of Information of Germany
- Personal Data Breach Severity Assessment Methodology

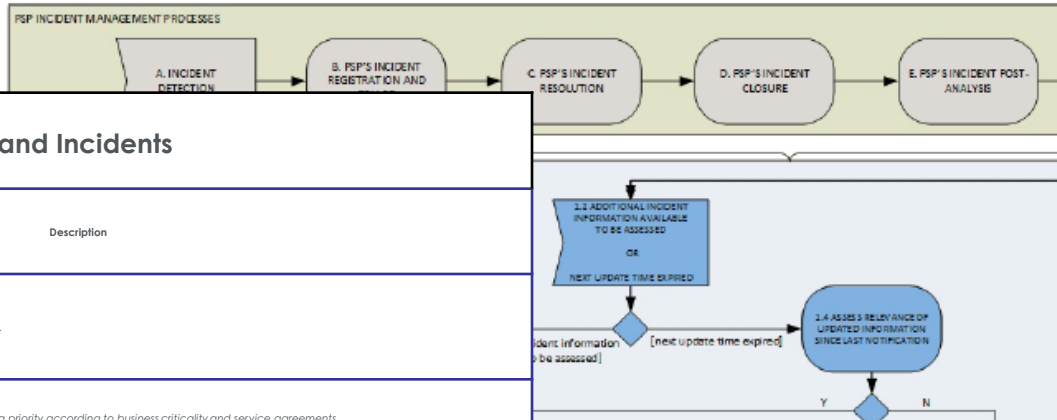
Strumenti

Ci sono buone pratiche
per gestire gli incidenti?


EBA/CP/2016/23
07 December 2016

Consultation Paper

on draft Guidelines on major incidents reporting under Payment Services Directive 2



DSS02 - Manage Service Request and Incidents

DSS02 - Management Practices	Description
DSS02.01 - Define incident and service request classification schemes.	*Define incident and service request classification schemes and models.*
DSS02.02 - Record, classify and prioritise requests and incidents	*Identify, record and classify service requests and incidents, and assign a priority according to business criticality and service agreements.*

Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie

Con istanze rivolte all'Autorità, numerosi interessati hanno dichiarato di essere venuti a conoscenza che dati personali a loro riferiti (in specie, informazioni bancarie), conservati nei data base di alcune banche con le quali avevano instaurato rapporti contrattuali, erano stati oggetto di ***indebito accesso****, verosimilmente da parte di alcuni dipendenti, i quali, successivamente,* ***li avrebbero comunicati a terzi*** *che* ***li avrebbero utilizzati per scopi personali*** *e, segnatamente, in vista di una loro produzione in giudizio (di norma, in separazioni giudiziali e procedure esecutive, in particolare, in pignoramenti presso terzi).*

GDPR

«violazione dei dati personali»: *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica,* ***la divulgazione non autorizzata*** *o* ***l'accesso ai dati personali*** *trasmessi, conservati o comunque trattati;*

BANCO BPM

Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie

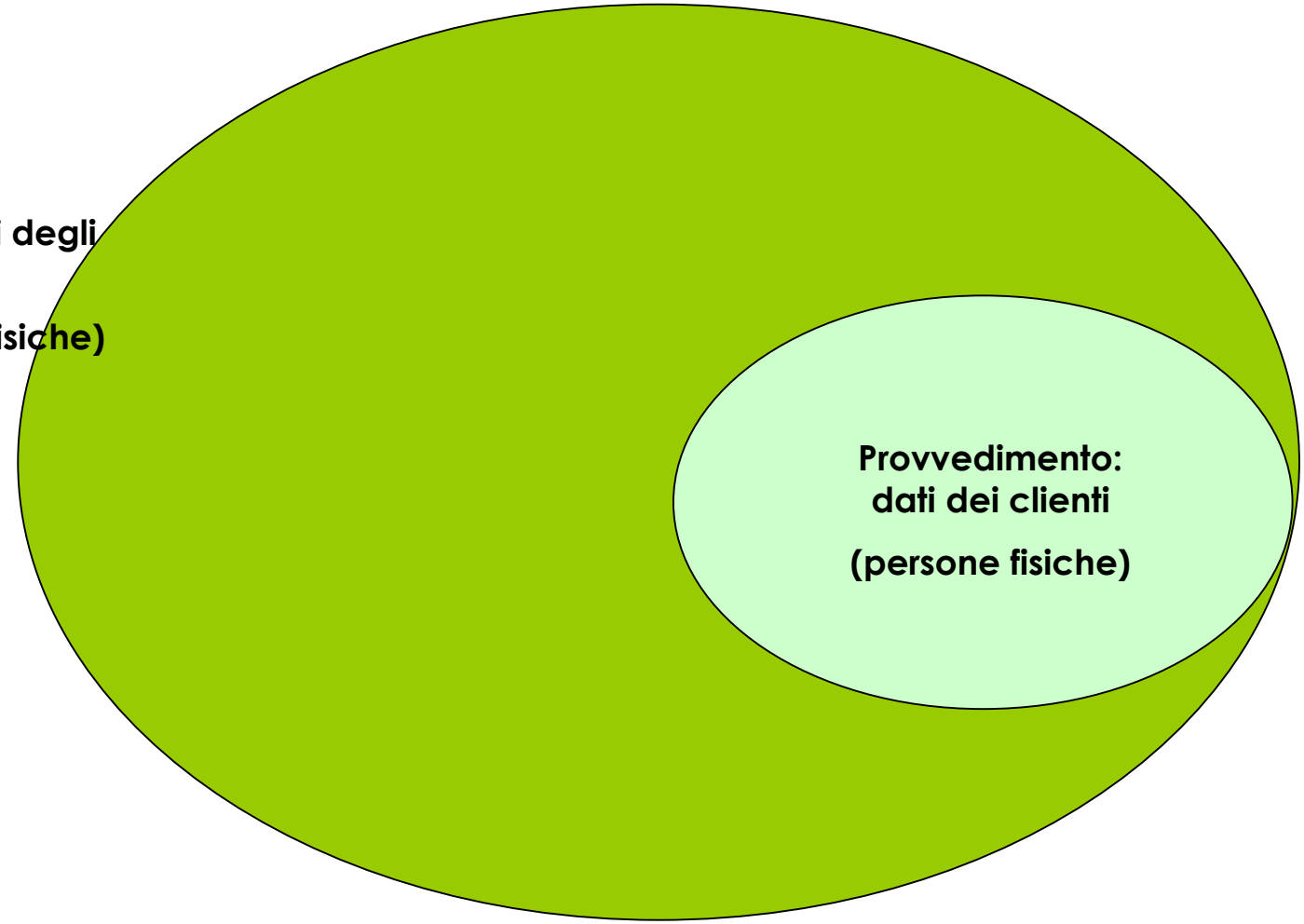
PRESCRIZIONI in un'ottica PbD

Al riguardo, nel prendere atto dell'assenza di disposizioni normative in tale ambito, si ritiene opportuno prescrivere alcune misure in ordine a:

- *"tracciamento" degli accessi ai dati bancari dei clienti;*
- *tempi di conservazione dei relativi file di log;*
- *implementazione di alert volti a rilevare intrusioni o accessi anomali ai dati bancari, tali da configurare eventuali trattamenti illeciti;*

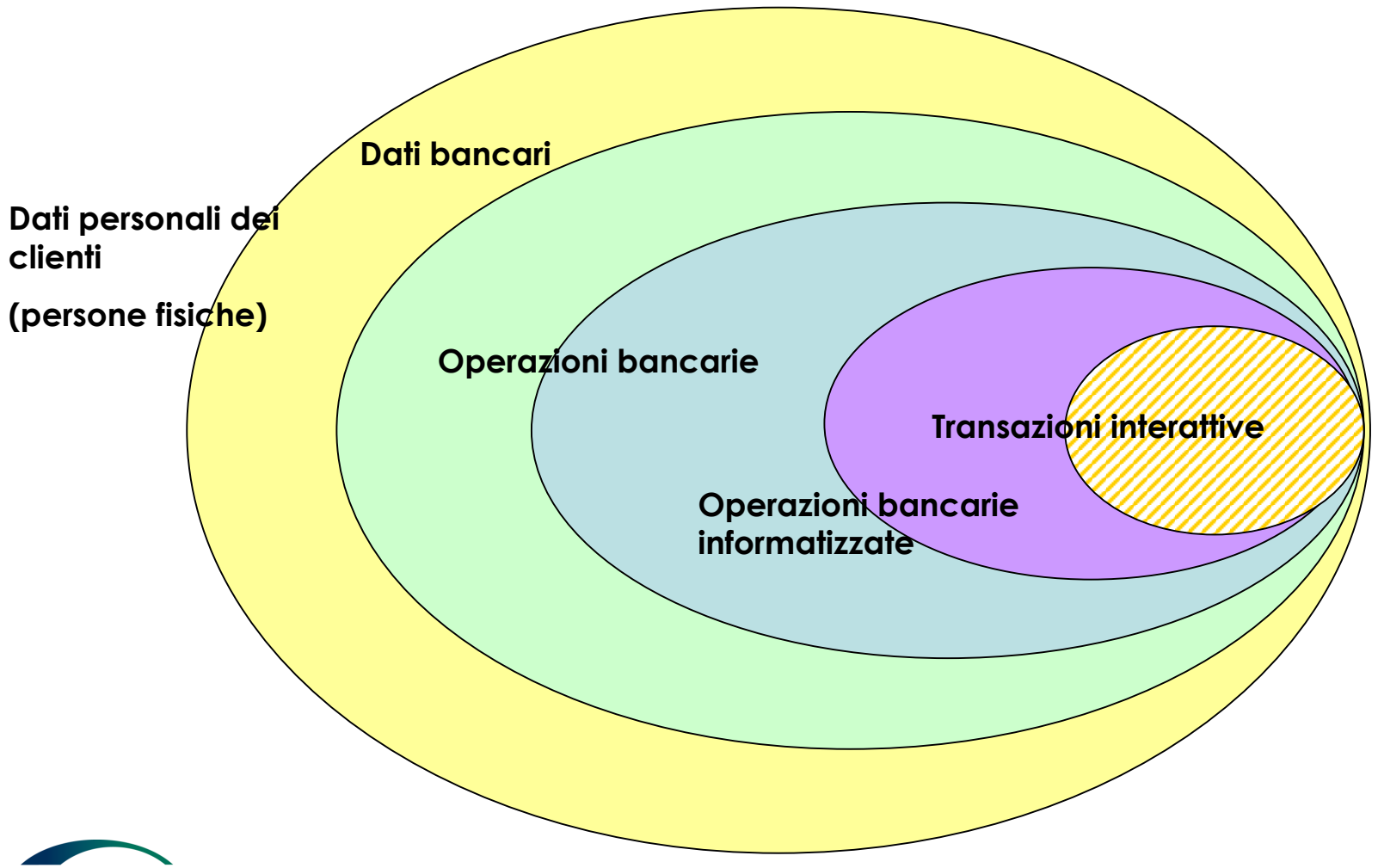
BANCO BPM

Il limite del provvedimento in ottica GDPR



BANCO BPM

Il limite del provvedimento in ottica GDPR



BANCO BPM

Il limite del provvedimento in ottica GDPR

Limitandoci a considerare l'ambito della clientela chi sono gli **interessati**:

- **clienti (persone fisiche)**
- potenziali clienti
- soggetti (persone fisiche) che operano per conto di clienti persone giuridiche
- soggetti (persone fisiche) che operano per conto di clienti persone fisiche
- soggetti (persone fisiche) che effettuano/ricevono transazioni nei confronti/dai clienti
- soggetti collegati ai clienti con cui la banca interagisce (ad esempio dipendenti dei clienti)

BANCO BPM

Possibili misure preventive alla violazione di dati personali

- Limitare l'accesso ai soli dati necessari
  - Corretta profilazione degli utenti
  - Corretta predisposizione degli spazi
  - Corretto uso degli strumenti promiscui
  - Corretta impostazione e gestione dei documenti
  - …
- Monitoraggio
  - Log ed alert
- Policy
  - Classificazione dei dati
  - Regolamentazione degli strumenti di comunicazione
  - …

BANCO BPM

Sicurezza: resilienza e continuità operativa

BANCO BPM

GDPR: Resilienza e continuità

GDPR - *Articolo 32* **Sicurezza del trattamento**

1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la **resilienza dei sistemi e dei servizi di trattamento**;
- **la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;**
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

BANCO BPM

Principi di sicurezza

Sicurezza del trattamento		
	Pseudonimizzazione	
	cifratura	
assicurare la continua …	riservatezza	…dei sistemi e dei servizi che trattano i dati personali;
	integrità	
	disponibilità	
	resilienza	
ripristinare tempestivamente in caso di incidente fisico o tecnico	disponibilità	
	accesso	
procedura per	provare, verificare e valutare	L'efficacia delle misure tecniche e organizzative

BANCO BPM

285: Resilienza e continuità

Circolare 285

le architetture sono disegnate in considerazione dei profili di sicurezza informatica delle applicazioni ospitate, tenendo conto di tutte le risorse ICT e di supporto interessate (alimentazione elettrica, impianti di condizionamento, ecc.); a tale riguardo, l'intermediario valuta la necessità di predisporre piattaforme particolarmente robuste e ridondate (ad es., applicando il principio del *no single point of failure*) volte a garantire l'**alta disponibilità** delle applicazioni maggiormente critiche, in sinergia con le procedure e il sistema di *disaster recovery;*

BANCO BPM

285: Requisiti per la continuità operativa

SEZIONE I

DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

La crescente complessità dell'attività finanziaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio richiedono che gli operatori rafforzino l'impegno a garantire adeguati livelli di continuità operativa.

A tal fine, essi adottano un approccio esteso che, partendo dalla identificazione dei processi aziendali critici, definisca per ciascuno di essi presidi organizzativi e misure di continuità operativa commisurati ai livelli di rischio.

Le concrete misure da adottare tengono conto degli standard e *best practices* definiti a livello internazionale e/o definiti nell'ambito degli organismi di categoria.

BANCO BPM

Grazie per l'attenzione

*Le affermazioni e le opinioni espresse nel presente documento **sono esclusivamente dell'Autore** e non vincolano in alcun modo le organizzazioni di appartenenza*

BANCO BPM