

# *Protezione dei dati, privacy e sicurezza informatica*

*Un nuovo approccio ai doveri privacy*

Avv. Martino Sforza  
[\*\*\*martinosforza@whitecase.com\*\*\*](mailto:martinosforza@whitecase.com)

---

Milano, 17 ottobre 2018



**PROBONO**  
ITALIA

# Perché il GDPR è rilevante? ... anche per gli enti no profit

- Organismi Volontariato, Associazioni Promozione Sociale, Enti del Terzo Settore, Imprese/Cooperative Sociali, Reti associative, ecc.
- Raccolgono e utilizzano dati personali
  - e.g., soci, associati, beneficiari, donatori, dipendenti, collaboratori esterni, destinatari di newsletter o mailing list (campagne *fundraising*)
- Anche particolari categorie di dati (dati sensibili, giudiziari)
- Alcune eccezioni

# Perché il GDPR è importante? ... anche per gli enti no profit



# Autoregolamentazione



# Alcuni esempi...



- 20 giugno 2018: BT sanzione GBP 77 mila per invio di 5 milioni di email spam per promuovere iniziative di beneficenza
- 17 luglio 2017: sanzioni GBP 171 mila nei confronti di 13 enti no profit
- Dicembre 2016: due importanti enti no profit sanzionati
  - Cessione illegittima di dati personali ed altre violazioni (wealth screening, profilazione dei donatori)

<https://ico.org.uk/your-data-matters/charity-fundraising-practices/>

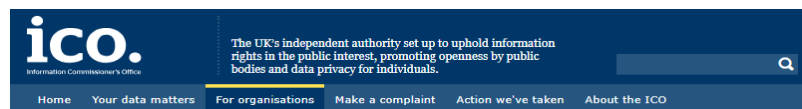
- Dicembre 2017 - Febbraio 2018: indagine conoscitiva dell'ICO su 8 enti no profit per verificare lo stato di implementazione delle principali misure in materia di protezione dei dati personali

<https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2259675/charities-audit-201808.pdf>

# Perché il GDPR è rilevante? ... anche per gli enti no profit

- Alcuni esempi di informazioni a disposizione degli enti no profit sul sito dell'ICO.

<https://ico.org.uk/for-organisations/charity/>



For organisations /

## Charity

### GDPR FAQs

Can I have specific guidance for charities? As a small charity what do I have to do to ensure we comply with the GDPR? These are just a couple of questions we have been getting from charitable organisations about the new data protection law.

[Our FAQs document answers these questions and many more](#)

### Small charities

The ICO has produced a package of tools and resources to help organisations, from sole traders to medium sized organisations, comply with their legal obligations under the new law that came in on 25 May 2018.

These resources include:

- a [micro business resource page](#);
- a [guide to the GDPR](#), which includes basic guidance and checklists;
- a number of data protection self- assessment checklists; and
- an [advice helpline for small organisations](#).

### Institute of Fundraising and Fundraising Regulator guidance, co-badged by the ICO

The Institute of Fundraising (IoF) and the Fundraising Regulator have released guidance on the GDPR which has been reviewed and co-badged by the Information Commissioner's Office.

[Fundraising Regulator website - GDPR and charitable fundraising guidance briefings](#) External link

### Fundraising and Regulatory Compliance Conference

The Fundraising and Regulatory Compliance Conference was aimed at helping charities and other fundraising groups comply with the law and was held at Manchester Town Hall on Tuesday 21 February.

For organisations /

## Guide to the General Data Protection Regulation (GDPR)

Share Download options

Search this document

### Introduction

What's new

Key definitions

What is personal data?

Principles

Lawfulness, fairness and transparency

Purpose limitation

Data minimisation

Accuracy

Storage limitation

Integrity and confidentiality (security)

Accountability principle

Lawful basis for processing

Consent

Contract

Legal obligation

Vital interests

Public task

Legitimate interests

### Introduction

The Guide to the GDPR explains the provisions of the GDPR to help organisations comply with its requirements. It is for those who have day-to-day responsibility for data protection.

The GDPR forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018). The main provisions of this apply, like the GDPR, from 25 May 2018.

This guide refers to the DPA 2018 where it is relevant includes links to relevant sections of the GDPR itself, to other ICO guidance and to guidance produced by the EU's Article 29 Working Party - now the European Data Protection Board (EDPB).

We intend the guide to cover the key points that organisations need to know. From now we will continue to develop new guidance and review our resources to take into account what organisations tell us they need. In the longer term we aim to publish more guidance under the umbrella of a new Guide to Data Protection, which will cover the GDPR and DPA 2018, and include law enforcement, the applied GDPR and other relevant provisions.

### Further reading

Data protection self assessment toolkit

For organisations

For a more detailed understanding of the GDPR it's also helpful to read the guidelines produced by the EU's Article 29 Working Party - which has now been renamed the European Data Protection Board (EDPB). The EDPB includes representatives of the data protection authorities from each EU member state, and the ICO is the UK's representative. The ICO has been directly involved in drafting many of these. We have linked to relevant EU guidelines throughout the Guide to GDPR.

# Le principali novità ....

**1) Consolidamento  
diritti e garanzie  
interessati**

**2) Valorizzazione  
ruolo autorità di  
controllo**

**3) Nuovo approccio  
ai doveri**

# Le principali novità del regolamento ....

## 1) Consolidamento dei **diritti** e delle **garanzie degli interessati**

- Consenso e informativa
- Accresciute garanzie di trasparenza
- Nuovi diritti (e.g., portabilità, diritto all'oblio)

## 2) Valorizzazione del **ruolo delle autorità di controllo**

- Nuovo ambito di applicazione territoriale
- *One-stop-shop* e cooperazione e assistenza reciproca
- Nuovo regime sanzionatorio (fino a **4% fatturato globale o EUR 20 milioni**)

## 3) **Nuovo approccio ai doveri *privacy***

- *Accountability, Privacy by Design e by Default*, certificazioni, codici di condotta, misure di sicurezza

# Nuovo approccio ai doveri privacy

- Il principio dell'*Accountability*
  - Passaggio da una concezione **formale** di adempimento ad un approccio **sostanziale**
  - **Documentabilità** delle scelte in merito alle misure adottate
  - Logica di maggior **responsabilizzazione** del titolare/responsabile
  - Dimostrazione di conformità attraverso:
    - Privacy **by design/ by default**
    - Codici di Condotta, certificazioni, misure sicurezza
    - **Audit e Risk Assessment**

Accountability





# Privacy by Design (1)

- Metodologia basata su 7 punti:
  - 1) prevenire non correggere, cioè i problemi vanno valutati nella fase di **progettazione**
  - 2) privacy come impostazione di **default**
  - 3) privacy **incorporata** nel progetto
  - 4) massima funzionalità
  - 5) sicurezza durante tutto il ciclo del prodotto o servizio (**end-to-end**)
  - 6) visibilità e trasparenza
  - 7) centralità dell'utente



## Privacy by Design (2)

- Applicazione **pratiche**
  - Qualunque «applicazione, servizio o prodotto, basato sul trattamento dei dati personali»
- **Investimento** iniziale per:
  - massimizzare potenzialità e **valorizzare** lo sfruttamento dei dati personali
  - garantendo **livelli adeguati di compliance**



# Privacy by Default

- Misure tecniche e organizzative adeguate per garantire che siano trattati
- per **impostazione predefinita**
- **solo** i dati personali necessari per ogni specifica finalità del trattamento:
  - **quantità** dei dati personali raccolti
  - **portata** del trattamento
  - **periodo** di conservazione
  - **accessibilità**



# Codici di Condotta

- Indicano:
  - Modalità di **corretta applicazione** della normativa nel contesto del settore
  - Meccanismi di **monitoraggio**
- Adesione a Codice di Condotta rende più **semplice** e **agevole** il rispetto del Regolamento
- Elaborazione da parte di **Associazioni di Categoria**
  - Che ruolo avrà il Consiglio Nazionale del Terzo Settore?
- **Approvazione** da parte del Garante
- Controllo da parte di un **organismo esterno**

# Certificazioni

---

- La Certificazione:
  - su base **volontaria**
  - organismi di certificazione **accreditati**
  - durata massima di **3 anni**
- Elemento per **dimostrare** il rispetto degli obblighi previsti dal Regolamento.



# Trasferimento internazionale dei dati

- Opzioni esistenti pre-GDPR.
  - Consenso; Decisioni Adeguatezza (Svizzera); Privacy Shield; Standard Contractual Clauses (SCC); Binding Corporate Rules (BCR)
  
- Nuove opzioni:
  - Clausole Standard Nazionali; Codici condotta/certificazioni; Settori Specifici

# Misure di Sicurezza – cosa cambia

---

## □ **Flessibilità**

- Misure adeguate in base allo stato dell'arte, costi di attuazione, contesto e finalità del trattamento

## □ **Accountability**

- *«misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio» - e.g.,:*
  - pseudonimizzazione
  - cifratura
  - assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi
  - capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente
- Adesione a **Codici Condotta** e **Certificazioni**



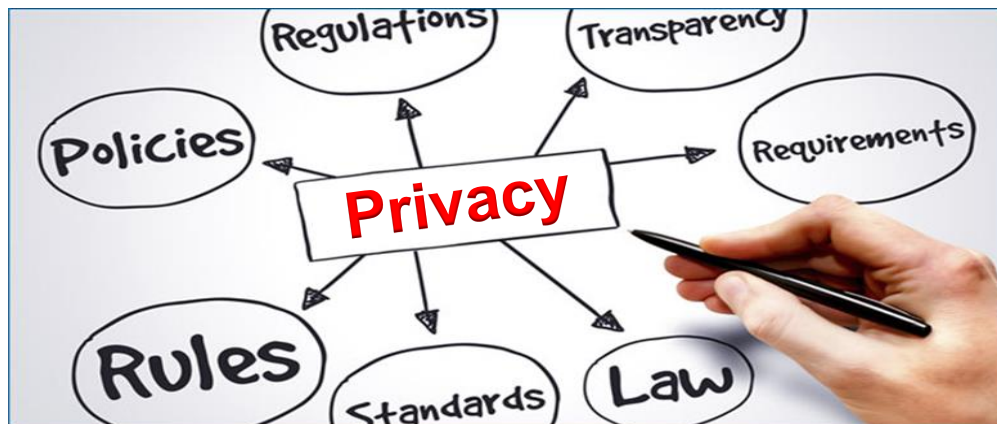
# Misure di Sicurezza – normativa NIS

- Obblighi per Titolare e Responsabile
- Coordinamento con Direttiva 1148/2016/UE sulla sicurezza di reti e sistemi informativi (NIS)
  - Decreto Legislativo 18 maggio 2018, n. 65
    - (entrato in vigore il 24 giugno 2018)
    - Ambito di applicazione analogo a quello della Direttiva:
      - ✓ energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile e infrastrutture digitali; motori di ricerca, servizi cloud e piattaforme di commercio elettronico
    - Nei rapporti tra enti no profit e soggetti attivi nei suddetti settori, necessità di verificare conformità a GDPR / Codice Privacy e Direttiva NIS / decreto di recepimento





# Audit e Risk Assessment – Quali step?



1. Identificare aree sensibili
2. Verifica *gap analysis*
3. *Struttura organizzativa Privacy*
4. Creazione *Check-list* e procedure
5. Verifica e Controllo
6. Attività Formative