International Differences in Data Protection: U.S. and Italy

In today’s digital economy, understanding the international differences in data protection is essential for safeguarding individual privacy, maintaining trust in digital services, and avoiding economic harm. This article outlines the overarching disparities between data protection laws between Italy and the U.S., highlighting how these varying frameworks impact regulatory compliance, data handling practices, and consumer rights across both regions.



Data Protection Frameworks in Italy



The **General Data Protection Regulation (GDPR)** is one of the most comprehens

ive and robust data protection laws globally, providing a cohesive framework fo

r
pr
oc
es
si
ng
pe
rs
on
al
da
ta
ac
ro
ss
th
e
Eu
ro
pe
an
Un
io
n
(E
U)
.
En
fo
rc
ed
si
nc
e
Ma
y
25

, 2018, the GDPR applies to all organizations that operate within the EU, offe

r
go
od
s
or
se
rv
ic
es
to
EU
ci
ti
ze
ns
,
or
mo
ni
to
r
th
e
be
ha
vi
or
of
in
di
vi
du
al
s
wi
th
in

the EU. Unlike U.S. regulations, the GDPR's scope includes non-profit organizati

ons, emphasizing that personal data protection is universal. It defines personal da

ta
br
oa
dl
y
as
an
y
in
fo
rm
at
io
n
re
la
te
d
to
an
id
en
ti
fi
ab
le
in
di
vi
du
al
,
en
su
ri
ng
wi

de-ranging protections for data subjects.

In Italy, the **Italian Privacy Code** (Legislative Decree n. 196/30 June 2003), modified by Legislative Decree n. 101/10 August 2018, implements GDPR provisions into national law. The Italian Privacy Code includes specific provisions, such as Title X, which incorporates the **e-Privacy Directive** (Directive 2002/58/CE). This directive regulates electronic communications and tracking technologies, including cookies, and ensures that data privacy extends to data exiting Italy's borders. Recently in June 2021, Italy updated its guidelines for tracking tools, such as cookies.

Key Principles of GDPR in Italy

1. **Data Minimization**: Collect only necessary data.

2. **Storage Limitation**: Retain data only as long as necessary.
3. **Accountability**: Organizations must demonstrate compliance.
4. **Accuracy**: Ensure data is accurate and up-to-date.
5. **Integrity and Confidentiality**: Protect data from unauthorized access and breaches.
6. **Purpose Limitation**: Data must be collected for specified, legitimate purposes.
7. **Lawfulness, Fairness, and Transparency**: Data processing must be lawful, fair, and transparent to data subjects.

Italian Data Protection Authority

The Italian Data Protection Authority, known as Garante Privacy, is responsible for the enforcement of the General Data Protection Regulation (GDPR) in Italy, the oversight of the implementation of national laws transposing the e-Privacy Directive, and the enforcement of the Personal Data Protection Code (Legislative Decree 196/2003) as amended by Legislative Decree No. 101 of August 10, 2018. Pursuant to Article 82 of the GDPR, data subjects harmed by violations can seek compensation from the data controller or the data processor. Additionally, in cases of large-scale regular and systematic monitoring or large-scale processing of special categories of data, the data controller or the data processor must appoint a Data Protection Officer (DPO).

Rights of Data Subjects in Italy



1. **Right to Access**: Individuals can request copies of their personal data.
2. **Right to Rectification**: Correct inaccuracies in personal data.
3. **Right to Erasure (Right to be Forgotten)**: Delete personal data under certain conditions.
4. **Right to Object**: Object to data processing in certain scenarios.
5. **Right to Restrict Processing**: Limit the use of their data.
6. **Right to Data Portability**: Transfer data to another controller.
7. **Right to Withdraw Consent**: Revoke consent for data processing at any time.
8. **Right to Object to Marketing**: Opt-out of marketing communications.

U.S. Data Protection Frameworks



The **data protection framework in the U.S.** traditionally reflect a hands-off ap

proach, prioritizing commercial success overstring ent data privacy, though this

mindset is gradually evolving. Unlike Italy’s comprehensive GDPR, the U.S. la

cks a uniform federal data privacy law and instead relies on sector-specific

regulations and a patchwork of state laws. Notable sector-specific laws incl

ud
e
th
e
He
al
th
In
su
ra
nc
e
Po
rt
ab
il
it
y
an
d
Ac
co
un
ta
bi
li
ty
Ac
t
(H
IP
AA
),
wh
ic
h
sa

fe
gu
ar
ds
se
ns
it
iv
e
he
al
th
ca
re
in
fo
rm
at
io
n,
an
d
th
e
Gr
am
m-
Le
ac
h-
Bl
il
ey
Ac
t
(G
LB

A), which mandates financial institutions to protect consumer information. At th

e
st
at
e
le
ve
l,
la
ws
li
ke
th
e
Ca
li
fo
rn
ia
Co
ns
um
er
Pr
iv
ac
y
Ac
t
(C
CP
A)
an
d
it
s
su
cc

esso r, the **California Privacy Rights Act (CPRA)**, provide broad rights to access

, delete, and opt-out of the sale of personal data. Other states have followed su

it with their own regulations, such as the **Virginia Consumer Data Protection Act (V**

CDPA), Colorado Privacy Act (CPA), Connecticut Data Privacy Act (CDPA), and th

e **Utah Consumer Privacy Act (UCPA).**

Key Principles of U.S. Data Protection Laws

Key principles under these U.S. frameworks include an opt-out basis for data collection, where user data is automatically collected unless they choose to opt-out. Consumer rights typically cover the right to opt-out of the sale or sharing of personal information, access and delete personal data, and correct inaccuracies. Enforcement of these laws is primarily handled by state attorneys general, with penalties for non-compliance ranging from $2,500 to $20,000 per violation. Notably, California’s CCPA uniquely provides consumers with the right to seek statutory damages, adding an additional layer of accountability for businesses.

Key International Differences in Data Protection: Italy and the U.S.

- **Scope**
  - **Italy's Broad Scope:** Applies to any organization established in Italy, offering products or services in Italy, or monitoring the behavior of Italy data subjects.
  - **U.S. State Laws' Narrow Scope:** Apply to companies within specific states or meeting certain thresholds (revenue, data volume) and does not include non-profits.



- **Consent Requirements**
  - **Italy's Opt-In Consent**:
    - Businesses must obtain explicit consent before collecting data.
  - **U.S. State Laws' Opt-Out Consent**:
    - Businesses can collect data until consumers opt-out.

- **Non-Compliance**

- **Italy’s High Penalties:**
  - Standard Violations: Up to €10 million or 2% of annual global turnover.
  - Severe Violations: Up to €20 million or 4% of annual global turnover.
  - Data subjects can claim compensation for material or non-material damage from data controllers or data processors.

- **U.S.’s Lighter Penalties:**
  - Range from $2,500 to $20,000 per violation.
  - Consumers generally cannot seek statutory damages with the exception of the CCPA

Most significantly, data protection and privacy in Italy is a fundamental right while it is not considered a fundamental right in the U.S.

Adapting to the Evolving International Differences in Data Protection

Navigating the complexities of data protection in the EU highlights the critical need for businesses to stay informed and compliant with evolving regulations. Ongoing issues, such as the transfer of data to jurisdictions outside the EU—like the U.S.—remain contentious, particularly given the international differences in data protection. Additionally, the increasing use of artificial intelligence presents new challenges, requiring updates to GDPR and related directives to address the ethical and privacy implications of AI. For businesses operating across these regions, staying compliant

not only mitigates legal risks but also helps maintain consumer trust and competitiveness in a data-driven economy. A.L. Assistenza Legale offers expert guidance to navigate these challenges, ensuring your company remains compliant and resilient in the face of evolving data protection laws.