

CPDP 2026
20 de mayo de 2026,
desde las 11:50 hasta las 13:05.
Lugar: The Grande Halle.

TRANSPARENCY BY DEFAULT:
an Internet Transparency Code of Practice

Moderador: Peter KIMPIAN (CoE)
Mark LIZAR (Canada Transparency Lab)
Jan SHALLABOECK
Peter KITS
Ana BRIAN NOUGRERES (UNSRP)

Distinguished colleagues,
Delegates,
Friends,

It is an honor
to address this panel today
at CPDP 2026,
as we convene,
in the Grande Halle.

To discuss the mechanics of operational transparency,
we must begin
by anchoring our technical discourse in its true purpose:

the protection and
the promotion of human dignity in the digital age.

In my capacity as the United Nations Special Rapporteur on the Right to Privacy,
I observe a world
where the traditional concept of "borders"
has been rendered almost obsolete
by the relentless flow of data.

We are no longer dealing with simple point-to-point transfers;
we are operating
within a borderless digital ecosystem
characterized by multi-party chains of controllers,
processors, and
AI service layers
that span the globe.

In this environment,
the right to privacy
is not merely an isolated legal provision;
it is a fundamental human right
that serves as a "gateway" or
as a prerequisite for the exercise of other essential freedoms,
such as the freedom of expression,
association,
and belief.

However,
this borderless nature
presents a profound paradox.

While technology transcends national boundaries,

our human rights protections
often remain fragmented,
struggling to keep pace
with the velocity and complexity of global data processing.

We see individuals and regulators
frequently unable to determine
—until long after the processing has begun—
who is truly accountable for their data,
what specific purpose is being pursued,
or what legal authority is being relied upon.

This lack of clarity
creates a systemic vulnerability.

When personal data
moves through opaque international channels
without clear governance,
the individual loses agency, and
the very fabric of trust
that should underpin our digital society
begins to fray.

The "trust us" posture
currently adopted by many actors
—where digital identification is demanded before accountability can even be inspected—
is not only a technical risk; it is a human rights challenge.

Therefore,
the imperative is clear.

We must move beyond a reactive stance and

establish a proactive framework
where transparency is not an afterthought
but a default operational requirement.
This is the foundation
upon which we must build
a world where the protection of the right to privacy
is as seamless
and as global
as the data flows it seeks to govern.

Only by ensuring
that governance models do not collide
but rather coalesce around shared human rights standards,
can we truly safeguard the individual
in this complex digital landscape.

In the contemporary digital landscape,
a standard interaction
often begins with a demand, and that demand is:
"Identify yourself."

Whether it is a login,
a biometric scan,
or the creation of a profile,
the individual
is required
to surrender their digital identity
as a prerequisite for service access.

However,
these digital identification demands
are

frequently
introduced at the very beginning of an interaction.

We are asked to engage in a leap of faith,
providing our most personal identifiers
based on abstract promises
that the backend processing is lawful and secure.

Yet,
as personal data moves through multi-party chains of controllers,
processors,
platforms,
identity providers,
and AI service layers,
the reality is far more opaque.

In such complex environments,
governance models often collide,
leaving a trail of data that is difficult to track or verify.

This model is
not only a technical shortcoming
but a systemic failure in governance.

It forces regulatory intervention to be reactive
—waiting for a breach
or a complaint
to investigate what happened long after the fact.

To move forward,
we must deconstruct this paradigm.

We must define
a new standard of "Transparency"
that specifies
exactly
what must be inspectable
before identification is demanded and
before any transfer occurs.

By embedding transparency and governance up front,
we enable regulatory intervention
to become proactive instead of reactive.

By requiring evidence artefacts
that make oversight scalable,
we can transition
from a model of blind trust
to one of verifiable accountability.

At this point,
as we have deconstructed the inherent risks of the "trust us" paradigm,
the question that naturally arises is:
upon what foundation
do we build a better alternative?

To address the systemic vulnerabilities
created when different governance models collide across digital borders,
we need a robust,
internationally recognized legal framework.

I propose
a practical approach
that is firmly grounded in Council of Europe Convention 108+.

In the actual fragmented landscape,
the need for a universally understood legal baseline
appears as paramount.

Convention 108+
serves as this exact legal cornerstone.

It provides
the necessary normative foundation
to ensure that fundamental human rights,
particularly the right to privacy,
are not lost in translation
or diluted as data crosses jurisdictional lines.

By relying on Convention 108+,
we are not merely debating abstract principles;
we are
setting the stage to introduce
a common structure
for implementing a "Transparency by Default" code of practice for transfers and
a digital identification management.

The modernized Convention
empowers us to demand that
accountability is a structural prerequisite,
not an afterthought.

It provides
the explicit legal mandate
to rigorously define what must be inspectable

before digital identification is demanded
and before any cross-border transfer occurs.

Convention 108+
gives us the normative weight
to challenge and change this unacceptable status quo.

Furthermore,
anchoring our operational transparency strategies
in Convention 108+
is a catalyst for modern digital governance
risk and compliance.

Embedding transparency and governance up front
enables regulatory intervention to shift
fundamentally—following it to become
proactive,
instead of reactive.

By establishing this legal cornerstone,
we open up multi-lateral capacities for governance
to enable cross border flows
for a common wealth sized market.

Ultimately,
Convention 108+
bridges the gap between
high-level human rights imperatives
and the scalable,
operational standards required to protect privacy in our hyper-connected world.

Now, going from principles to practice,

having established Convention 108+ as our indispensable legal cornerstone,
we must now
confront
the defining challenge of our era:
how do we translate these profound legal principles
into tangible, operational reality?

Legal text,
no matter how rigorously drafted,
cannot execute code
or parse data packets on its own.

It requires technical translation to be effective on the ground.

This brings us to the core of our discussion today.

We are proposing
a practical "Operational Transparency" code-of-practice approach.

This approach is fundamentally grounded
in the rights established by Convention 108+
and is actively being operationalized
through ISO/IEC WG 5 standardisation work.

Our primary aim
is to introduce
a common structure
for implementing a Transparency by Default code of practice
for transfers
and a digital identification management.

To achieve this,

we must shift the timeline of compliance.

We must definitively
define
what must be inspectable
before identification is demanded
and before transfer occurs.

To bridge
this gap
between legal requirement and technical execution,
the ISO/IEC WG 5 standardization work
focuses on the creation and
implementation of specific "evidence artefacts".

These artefacts
are designed
to capture and communicate
the governance framework
attached to a data flow.

By attaching standardized,
verifiable evidence to data transfers,
we eliminate
the blind spots
where individuals and regulators
often cannot determine who is accountable,
what purpose is pursued,
what authority/justification is relied on,
and what onward disclosures occur
until long after processing is underway.

The implications
of this shift for modern digital governance risk
and compliance are profound.

When we effectively embed transparency and governance up front,
it entirely transforms the role of data protection authorities.

It enables regulatory intervention
to become proactive,
instead of reactive.

Regulators
will no longer be relegated
strictly to the role of digital archaeologists,
investigating breaches after the damage is done.

Instead,
they will be equipped to monitor the structural integrity of data processing frameworks in real-time.

This seamless integration of legal principles
and technical standards
opens up multi-lateral capacities for governance.

It provides
the necessary trust infrastructure
to securely enable cross border flows
for a common wealth sized market.

By turning operational transparency
from an aspiration into an ISO-backed reality,
we prove that robust privacy protection
and seamless global digital innovation

are not mutually exclusive, but deeply interdependent.

Closing Remarks

As we finish this presentation,
I want to leave you with a clear vision
of the future we are striving to build.

We have discussed
the urgent need to move away from the blind "trust us" posture
and recognized that
cross-border transfers are the critical junctures
where different governance models collide.

By grounding our approach in Convention 108+
and operationalizing it through the ISO/IEC WG 5 standardization work,
we are actively defining
what must be inspectable
before identification is demanded and
before transfer occurs.

This shift
is not merely a technical adjustment;
it is a fundamental transformation
of modern digital governance risk and compliance.

For far too long,
the protection of the right to privacy
has been a deeply reactive endeavor,
leaving authorities to clean up
after data has already been misused.

However,
when we embed transparency and governance up front,
it enables regulatory intervention to become proactive,
instead of reactive.

This means
empowering individuals and data protection authorities
with the necessary evidence artefacts
that make oversight truly scalable.

Our shared aim
is to introduce
a common structure
for implementing a Transparency by Default code of practice
for transfers
and a digital identification management.

I call upon the global community
—regulators,
technologists,
and civil society—
to champion this operational transparency.

We must demand
that digital systems are architected
to prove their compliance and accountability
at the very first point of interaction,
not after the data is already flowing through opaque,
multi-party chains.

Adopting this proactive stance
does not hinder technological progress.

On the contrary,
it opens up multi-lateral capacities for governance
to enable cross border flows
for a common wealth sized market.

It provides
the trust and legal certainty required
for a thriving global digital economy.

As the UN Special Rapporteur,
I firmly believe that
human rights and digital innovation
must advance in tandem.

Let us commit
to building a digital ecosystem
where privacy is the default,
where transparency is fully operationalized,
and where human dignity remains the indisputable center of
our shared digital future.

Thank you!