



Digital Policy Alert

Activity Tracker Handbook

Design choices, workflows, and codebook

An initiative of the

**St. Gallen
Endowment**

for Prosperity through Trade

Contents of the DPA Activity Tracker Handbook

This version: 5 October 2026, find the latest copy [here](#).

About the Digital Policy Alert	3
The first public inventory of laws and regulation affecting the digital economy	3
How to use the Digital Policy Alert	3
Get in touch with questions, suggestions, or comments	4
The DPA activity tracking priorities	4
The DPA reporting heuristic	4
The DPA reporting wild cards	4
Reduced tracking for non-binding regulations and civil lawsuits	5
The DPA activity tracking workflow	5
About the DPA Activity Tracker taxonomy	6
Our units of analysis: Interventions and events	6
Two taxonomies to address policy questions in detail	6
The Activity Tracking taxonomy at a glance	6
Information on the regulatory authority profile	7
Implementing jurisdiction	7
Implementation level	7
Government branch and government body	7
Information on the substance of regulatory change	9
Policy area and policy instrument	9
Data governance	9
Content moderation	9
Competition	10
Taxation	11
Intellectual Property	11
Labour Law	11
Authorisation, registration and licensing	12
Consumer protection	12
Design and testing standards	13
Other operating conditions	14
Foreign direct investment	14
International trade	14
Public procurement	15
Economic activity	16
Event type	17
Action type	18

About the Digital Policy Alert

The first public inventory of laws and regulation affecting the digital economy

Navigating the **dynamic landscape of the digital economy** can be challenging due to uncoordinated government regulations and the lack of international best practices. Worse, there is currently no international monitoring effort for laws and regulations affecting the digital economy. The Digital Policy Alert (DPA) aims to fill this evidence gap by offering publicly accessible, transparent, and timely documentation of policy and enforcement developments.

Launched in April 2021, our dedicated team has tracked over **14,705 policy changes** using a comprehensive tagging system for easy user discovery. Our data collection boasts:

1. **Extensive coverage:** G20 nations, EU member states, Switzerland, New Zealand, the Philippines, Singapore, Viet Nam, Thailand, and Chinese Taipei. Following the expansion to Africa, we cover Nigeria, Ghana, Rwanda, Morocco, Algeria, Kenya, Ethiopia, and Egypt.
2. **Broad policy scope:** Data governance, content moderation, competition, and more (see taxonomy below).
3. **Timeliness:** Daily tracking of developments since January 2020.
4. **All branches of government:** Legislation, executive orders, enforcement cases, and court decisions with general implications.
5. **Full policy lifecycle:** Tracking the proposal, deliberation, adoption, implementation, and revocation.
6. **Customisable presentation:** A rich tagging system for easy analysis of policy features.
7. **Independent verification:** All entries provide official sources and undergo a 2-step human review process.

How to use the Digital Policy Alert

The [DPA website](#) serves as a one-stop-shop to navigate global digital policy, with various **functionalities**:

- Each DPA entry provides a link to the original source, a brief human-written description, an overview of the full lifecycle and related developments, and the classification along the DPA taxonomy.
- On the [Activity Tracker](#), users can filter the DPA data along all taxonomy fields and export the full dataset.
- On the [Notification Service](#), users can subscribe to free, tailored e-mail notifications on new developments.
- Our [Threads](#) provide topical cuts of the data, providing both summary statistics and tailored data feeds.
- Our [Aggregate Dynamics](#) page visualises the empirical findings of the DPA in interactive fashion.

Our data serves a broad **audience**. Policymakers drafting digital policy use the DPA to understand regulatory approaches across the globe. For industry representatives, the DPA provides a snapshot of compliance rules in different markets and acts as an early warning system for new developments. Members of the research, media, and legal communities rely on the DPA to contextualise digital policy developments relevant to their work.

The DPA combines policy monitoring with **in-depth analysis**. Our flagship report on [Emergent Digital Fragmentation](#) and the [Digital Digest series](#) offer insights into the G20 nations' domestic digital policy landscape. Our report on [Data Governance Regulation in the G20](#) systematically compares domestic rules and their effect on fragmentation.

The DPA is a **policy transparency initiative** by the [St.Gallen Endowment for Prosperity through Trade](#). It leverages technology and policy monitoring expertise from its sister project, the [Global Trade Alert](#), established in 2009. Together, we are supporting innovation in the digital economy, empowering stakeholders with the knowledge they need to navigate the regulatory landscape, and fostering collaboration to prevent digital fragmentation.

Get in touch with questions, suggestions, or comments

This methodology ensures that the DPA remains a **precise and authoritative resource**, focusing on the most impactful regulations and legal decisions shaping the digital economy. It is designed to offer clarity and insight to policymakers, legal professionals, and industry stakeholders navigating the complex landscape of digital policy. Please direct open questions, comments or suggestions to info@digitalpolicyalert.org. We offer free website demonstrations on request.

The DPA activity tracking priorities

Our **reporting objective** is to provide users with the most important digital regulatory news every single day. The reporting priorities described below guide DPA analysts through the stream of incoming information.

The DPA reporting heuristic

Our **reporting priorities** yield a general ordering heuristic, not an unambiguous ordering rule. The priorities are multi-dimensional and should be understood as an algorithm that seeks to mimic the ranking overlap for a wide set of users. DPA analysts can use their good judgment on what DPA users need to see first.

The following **6 priority dimensions** are the components of the priority algorithm for what DPA users want to see:

1. The DPA focus countries are the G20 members, the EU and its member states, and Switzerland. We are currently expanding to Southeast Asia, starting with New Zealand, the Philippines, Singapore, Viet Nam, and Thailand.
2. We aggressively prioritise recent events over older events.
3. We prioritise the policy areas data governance, content moderation, competition and taxation.
4. We prioritise binding over non-binding regulatory events.
5. We prioritise implementing or revoking actions over deliberative actions.
6. We prioritise events that discriminate based on nationality.

The list above is ordered from most to least important, but it is unclear what the distance between the items is. Of the six, the first stands out to ensure that DPA coverage is always comprehensive for our focus countries.

The DPA reporting wild cards

There are also **5 wild cards**. Drawing a wild card means that DPA analysts report an event with high priority even though the trade-offs based on our usual heuristic would not warrant it. For example, one may invoke a wild card to argue that DPA users need to be notified about a sweeping AI regulation in a jurisdiction outside current DPA focus.

The current **DPA wild cards** are:

1. **High fragmentation risk** understood as policy instruments that can fracture the digital economy (almost) by design. Several policy instruments on the DPA have high fragmentation risk:
 - a. Localisation measures (data localisation, local operations, local content, investment in local content)
 - b. Cross-border data transfer regulation
 - c. Customs duties on electronic transmissions including data or content
 - d. Direct taxation of digital goods or services
2. **Media salience** understood as the amount of media attention nationally or worldwide. This can include media coverage for non-economic reasons such as cherished norms (e.g. privacy) or desired societal goods (e.g. inclusivity such as creating opportunities for SMEs, women, and other disadvantaged groups).
3. **Economic impact** understood as altering the terms of competition in a country or economic activity.
4. **Legal impact** understood as a significant legal barrier being raised or a significant (potential) reinterpretation of current regulatory practice in a country or region.
5. Significant (potential) changes to **international cooperation** on digital economy regulation that widen or ameliorate the fragmentation of the internet.

Reduced tracking for non-binding regulations and civil lawsuits

The DPA aims to be **exhaustive** in documenting all binding regulations within its purview. To focus our resource on those regulatory events most likely to shape the digital business environment, we limit our tracking of non-binding regulations as well as civil lawsuits. We do not exclude either since they may, in rare circumstances, shape the digital business environment as well.

The DPA tracks **non-binding, government-issued guidance**, classified as “outlines” in our taxonomy, specifically pertaining to compliance, implementation, and enforcement of existing or impending laws and regulations. It concentrates on directives that bear legislative weight, intending to map the trajectory of policy execution and the minutiae of regulatory adherence. However, it deliberately excludes non-binding pronouncements such as action plans or annual reports by agencies or parliamentary bodies. These types of documents, although possibly instructive, do not strictly delineate or enforce compliance with existing or impending legislation, and thus fall outside the purview of this monitoring effort.

While the DPA includes **civil lawsuits**, the approach differs from other developments. Only those civil cases that lead to rulings with broad implications for the digital economy are documented, starting from the ruling, and covering any subsequent appeals or decisions. An example for such a case is the Supreme Court decision in Google vs. Oracle which had implications for the interpretation of fair use with respect to source code.

The DPA activity tracking workflow

The DPA **workflow** combines human intelligence and technology to deliver verified data in an accessible format.

The DPA operates on a **newsroom model** to publish approximately 20 new entries every day.

- Every morning, our web crawlers collect relevant information from government sources across the world, producing our “leads.” Senior analysts complement these automated leads with manual research to ensure comprehensive coverage and then prioritise leads for integration into the DPA database.
- Throughout the day, junior analysts based around the globe process each lead by analysing the official source, coding the development using the DPA taxonomy, and summarising their findings in a brief description.
- In the afternoon, senior analysts review the official source, the coding, and the description of each lead.
- Before 6pm CET, executives do a second review and publish the DPA entry in time for our daily newsletter.

Several **precautions** in our workflow ensure the reliability of the DPA database:

- We rely exclusively on official government sources. This guarantees that our coverage is neutral.
- Our continuous tracking of governmental websites ensures that our reporting is not systematically influenced by the news cycle.
- We are a globally distributed team. This enhances our understanding of local developments and languages. Wherever our team does not cover a language, we rely on common translation applications.
- We build our own technology. The technology team at the St.Gallen Endowment builds the tools that enable the Digital Policy Alert’s monitoring, including the DPA website, the web crawlers that generate leads, and the machine learning models that underly our information sorting and chat interfaces.

About the DPA Activity Tracker taxonomy

Our units of analysis: Interventions and events

The DPA's primary unit of analysis is the “**intervention**” that represents the application of a policy instrument, such as the enactment of a new data protection rule or a content moderation requirement. Each intervention is meticulously catalogued with relevant details, including the policy area, policy instrument, and the responsible government body.

The DPA employs a **lifecycle approach** to monitor the entire journey of a regulatory intervention, from inception to revocation. This approach necessitates tracking “events” that mark lifecycle milestones such as the introduction, passage, signing, or implementation of a regulatory change. The events in the Digital Policy Alert (DPA) database provide date-specific information such as the relevant official source or a short summary of changes made compared to prior stages.

Two taxonomies to address policy questions in detail

The DPA taxonomy is a comprehensive framework designed to **systematically categorise and track** digital policy developments worldwide. This taxonomy enables users to slice through the dataset and only retrieve what is relevant to their use case. At the DPA, we distinguish between “Activity Tracking” and the “Detailed Mapping”.

The purpose of the **Activity Tracking** taxonomy is to capture the essential information necessary to most use cases and publish it alongside our daily updates. The purpose of the Detailed Mapping is to capture the nuances of regulations based on the official text and decompose it to make them comparable at a high level of detail across jurisdictions.

The taxonomy for the **Detailed Mapping** varies by policy area is published separately as it develops. Please consult our report on [Data Governance Regulation in the G20](#) (November 2023) for an illustration of the Detailed Mapping applied to data rules.

The Activity Tracking taxonomy at a glance

The DPA Activity Tracking team structures the information it collects along two **primary groups**:

1. **Information on the acting regulatory authority:** This section delves into the specifics of the entities responsible for implementing digital policies. It covers the:
 - a. Implementing Jurisdiction: The geographical and political scope of the authority.
 - b. Implementation Level: The local, national, or international level of the policy.
 - c. Government Branch: The specific branch of government involved in the policy action.
 - d. Government Body: The exact governmental department or agency responsible for the policy action.
2. **Information on the substance of the regulatory change:** This section focuses on the nature and scope of the regulatory actions themselves. It encompasses the:
 - a. Policy Area: The legal area of the policy.
 - b. Policy Instrument: The basic tools employed in the policy.
 - c. Economic Activity: The digital economic sector or activity affected by the policy.
 - d. Event Type: The legal nature and binding status of the policy.
 - e. Action Type: The specific action taken, such as the adoption, amendment, or repeal of the policy.

This taxonomy serves as a **vital tool** for regulators, policy professionals, and media, providing a clear and structured means to access and analyse digital policy data efficiently and effectively. Each section in the following handbook will offer a detailed description of these dimensions, including field values, descriptions, and examples.

Information on the regulatory authority profile

This section of the Digital Policy Alert (DPA) taxonomy is dedicated to illuminating the **entities behind digital policy initiatives**. This section provides a systematic breakdown of the various facets of the regulatory authorities, offering clarity on who is responsible for initiating, enacting, and enforcing digital policies.

Implementing jurisdiction

The implementing jurisdiction refers to the **geographical and political scope** within which a regulatory authority operates. The DPA names uses the official names of jurisdictions worldwide as used by the United Nations Statistics office. For subnational units, we use the common name in English language.

Implementation level

The implementation level categorises policy based on its **reach**. This dimension is essential for identifying the scope and scale at which digital policies are implemented. It distinguishes whether a policy is local, regional, national, or international. Understanding the implementation level of a policy aids in assessing its impact and relevance across different geographical areas.

The different **implementation level** values used by the DPA team are:

- Supranational: Regulations formulated by a supranational entity that transcend national boundaries. *Example: European Union (EU) directives.*
- National: Policies implemented at the country level. These are standard regulations that apply within the boundaries of a single economy. *Example: The United States' Federal Communications Commission (FCC) regulations.*
- Subnational: Policies enacted at a level below the national government, such as state or provincial regulations. *Example: Data privacy regulations specific to the state of California.*
- Bi- or Plurilateral Agreement: Policies formed as a result of agreements between two or more countries, but not extending to the level of multilateral organisations. *Example: Digital trade agreements between specific countries.*
- Multilateral Agreement: Policies established through global or quasi-global agreements. *Example: A World Trade Organization (WTO) level agreement on digital services.*

Government branch and government body

The government body and branch describe the **originator** of a policy. The government branch dimension identifies the specific branch of government responsible for the policy. The DPA team distinguishes between the executive, legislature and judiciary branch. The government body dimension categorises the specific governmental departments, agencies, or offices responsible for digital policy actions. The legislature only has the parliament as body, while the judiciary is only split into court and supreme court, which makes final rulings. The executive is subdivided into several bodies.

The different **government branch and body** options available are:

- Legislature - Parliament: The legislative body responsible for creating and amending laws.
- Judiciary - Court: Courts at various levels that interpret laws and adjudicate legal disputes.
- Judiciary - Supreme Court: The highest judicial authority, providing final rulings on legal matters.
- Executive - Central Government: The central administrative authority responsible for overarching policy decisions and implementation.
- Executive - Data Protection Authority: The entity focused on enforcing data protection laws and regulations.
- Executive - Competition Authority: The body that oversees and regulates issues related to competition.
- Executive - Consumer Protection Authority: The authority responsible for safeguarding consumer rights.

- Executive - Central Bank: The monetary authority of a country.
- Executive - Tax Authority: The entity responsible for taxation policy and enforcement.
- Executive - Other Regulatory Body: A regulatory body not captured by the above.

Information on the substance of regulatory change

This section of the Digital Policy Alert (DPA) taxonomy provides a comprehensive overview of the various aspects of regulatory actions within the digital policy domain. It is structured to offer a detailed understanding of the **nature, tools, and scope** of regulatory initiatives.

Policy area and policy instrument

The policy area dimension organises each database entry by locating it in a broad **area of law**. The main policy areas are currently data governance, content moderation, competition, taxation, intellectual property, and labour law. Each policy area has its own instruments. The policy instrument details the tools or mechanisms employed by regulatory authorities to achieve their policy objectives.

Data governance

Data governance encompasses the set of policies that dictate the **management, use, and protection of digital information**. It involves regulations that define the rights of data subjects, the obligations of data handlers, the procedures for data processing, and the measures for data security. This area of law addresses the complexities of information flow in the digital age, including how data is collected, stored, shared, and secured across various platforms and national borders.

The DPA team currently distinguishes between the following data governance policy instruments:

- Data protection regulation: Rules defining the rights of individuals regarding their personal data and setting responsibilities for data processors and controllers. *Example: The EU General Data Protection Regulation (GDPR) provides individuals within the rights to access, correct, and delete their personal data.*
- Cross-border data transfer regulation: Rules establishing conditions under which personal data can be transferred across national borders, often to maintain domestic data protection standards. *Example: The Court of Justice of the EU's "Schrems II" decision invalidated the EU-US Privacy Shield, impacting the transfer of personal data from the EU to the US.*
- Data localisation requirements: Rules requiring data concerning a country's citizens or residents to be collected, processed, and stored within the country. *Example: The Chinese Personal Information Protection Law necessitates that certain personal data collected and generated in China be stored domestically.*
- Cybersecurity regulation: Rules requiring measures to secure data and digital infrastructures against cyber threats, including preventive, detective and reactive measures. *Example: The Chinese Cybersecurity Law mandates network operators to fortify information protection and report cybersecurity incidents.*
- Data protection authority governance: Rules establishing and managing the powers of national authorities that enforce data protection rules. *Example: Brazil established a new data protection agency to oversee and enforce its Law on General Data Protection (LGPD).*
- Government access to data: Rules governing the conditions under which government authorities can request, access, or use data held by private entities. *Example: The United States Foreign Intelligence Surveillance Act (FISA) Section 702 allows government agencies to access data on non-US persons located abroad for foreign intelligence purposes.*
- Data governance, nes: Unspecified data governance rules that affect the digital economy.

Content moderation

The domain of content moderation encompasses the regulatory measures directed at digital intermediaries regarding the **content they host, moderate, and disseminate**. This includes the obligations that platforms have to moderate user-generated content, the limitations imposed on the removal of content, and the upholding of "free speech" principles. It also covers the requirements for platforms to support local content through quotas and the remuneration of content creators, particularly in the context of news dissemination. The establishment or empowerment of agencies to oversee these aspects of digital content is also an integral part of this domain.

The DPA team monitors regulations applied to entities that intermediate content, such as platforms or over-the-top (OTT) service providers and does not include regulations for entities that produce their own content, such as online

newspapers. The focus here is on the unique regulatory challenges that arise from the digital delivery of content by intermediaries, as opposed to traditional content publishers.

The DPA team currently distinguishes between the following content moderation policy instruments:

- User speech right: Rules limiting the power of platforms to regulate speech and enhancing protections for users to express themselves online. *Example: US state-level "free speech" laws restrict the moderation and banning of political content on social media platforms.*
- Content moderation regulation: Rules obligating platforms to remove certain types of content, aimed at protecting public order or preventing harm. *Example: The UK Online Safety Act sets out a legal framework for digital platforms to remove harmful content.*
- Local content requirement: Rules mandating quotas of locally sourced content to support domestic creators and preserve cultural identity. *Example: The "Netflix Act" in Switzerland mandates a 30 per cent quota for European content on streaming platforms.*
- Investment in local content obligation: Rules for digital platforms or service providers to invest in or support the production of local content. *Example: The EU's Audiovisual and Media Services Directive requires streaming services to allocate a portion of their revenue to the production of locally made content.*
- Content moderation authority governance: Rules creating or modifying regulatory bodies to supervise digital content moderation practices. *Example: The EU Digital Services Act establishes of the "Board for Digital Services" under the to oversee moderation activities on large online platforms.*
- Content moderation, nes: *Unspecified content moderation rules that affect the digital economy.*

Competition

The competition policy area focuses on regulations that govern **competitive practices in digital markets**. These policies aim to prevent anti-competitive behaviour, ensure fair market conditions, and maintain a level playing field for all participants. This includes scrutiny of mergers and acquisitions that might lead to market consolidation, regulations against unilateral conduct that could abuse market power, and rules against anti-competitive agreements. Additionally, state aid control investigates how states support firms to maintain fair competition. The domain also extends to the governance of competition authorities and their jurisdictional powers, ensuring that they are equipped to address the unique challenges posed by the digital economy.

The DPA team currently distinguishes between the following competition policy instruments:

- Merger control regulation: Rules regarding the assessment and restriction of mergers between firms to prevent market consolidation. *Example: The UK Competition and Markets Authority blocked Facebook's acquisition of Giphy due to concerns over market dominance.*
- Unilateral conduct regulation: Rules addressing actions by large digital firms that could lead to the abuse of market power. *Example: South Korea amendment to the Telecommunications Business Act prohibits mandatory in-app purchasing systems.*
- Anti-competitive agreements regulation: Rules establishing boundaries on agreements between competitors to prevent collusive practices. *Example: The European Commission examined the Jedi Blue agreement between Alphabet and Meta, which allegedly gave Facebook an advantage in advertising agreements.*
- State aid control: Rules regarding the support that states provide to firms, ensuring such aid does not distort market competition. *Example: The EU State Aid rules set the framework for state aid.*
- Competition authority governance: Rules changing the jurisdiction of or creating new competition agencies. *Example: The German Bundeskartellamt's enforcement powers were expanded to conducting ex-ante investigations on digital companies.*
- Competition, nes: *Unspecified competition rules that affect the digital economy.*

Taxation

The taxation policy area addresses the **fiscal aspects of the digital economy**, focusing on how digital services and transactions are taxed domestically. This includes the imposition of direct and indirect taxes on digital services, such as digital service taxes, value-added taxes, and other forms of levies that apply to digital transactions and operations.

The DPA team currently distinguishes between the following tax policy instruments:

- Direct taxes including digital service taxes: Rules imposing taxes directly on the revenues or profits generated from digital services. *Example: The implementation of digital service taxes (DST) in countries like Canada and India, targeting revenues from specific digital services.*
- Indirect taxes: Rules regarding the application of existing indirect taxes, like value-added tax (VAT) or accommodation tax, to digital services. *Example: US state-level accommodation taxes on platforms like Airbnb.*
- Taxation, nes: Unspecified taxation rules that affect the digital economy.

Intellectual Property

The intellectual property policy area deals with the rules and regulations surrounding the **protection and management of creations of the mind** in the digital realm. This includes policies that address patents, copyrights, and other forms of intellectual property rights as they apply to digital content and innovations.

The DPA team currently distinguishes between the following intellectual property policy instruments:

- Patent protection regulation: Rules that define how patents are granted and enforced for digital inventions. *Example: The US Patent and Trademark Office current stance on not recognising AI as an “inventor” for the purposes of patent filings, which maintains the requirement for human inventorship in the patent system.*
- Copyright protection regulation: Rules governing the protection of copyrighted material in the digital environment. *Example: France’s law to regulate artificial intelligence through copyright*
- Content remuneration regulation: Rules regarding the compensation for content creators when their work is utilised on or by digital platforms. *Example: The Australian News Media and Digital Platforms Mandatory Bargaining Code requires platforms to come to a bargaining agreement with domestic news outlets for the reuse of their content.*
- Intellectual property, nes: Unspecified IP regulations outside the scope of patents and copyright that affect the digital economy.

Labour Law

Labour law encompasses policies that address the **rights, classification, and monitoring of workers** in the digital economy. This area is becoming increasingly important as the gig economy expands and technology further integrates into workplaces.

The DPA team currently distinguishes between the following labour law instruments:

- Worker classification or protection regulation: Rules defining the status of workers in the digital economy, distinguishing between traditional employees and independent contractors, or establishing worker protections. *Example: The Swiss Federal Supreme Court ruled that Uber drivers should be classified as employees to ensure they receive labour protections and benefits.*
- Worker monitoring regulation: Rules on how employers can monitor and analyse workers, often using algorithmic or automated systems. *Example: US state-level legislation prohibits the use of AI for worker surveillance to protect the privacy and autonomy of employees.*
- Labour law, nes: Unspecified labour rules that affect the digital economy.

Authorisation, registration and licensing

The registration and licensing policy area in the digital economy involves regulations that require digital businesses to obtain **official permission or fulfil certain conditions** to operate. This includes licensing requirements for specific

business models, registration mandates for particular types of digital operations, and authorisations for offering certain goods or services. These policies are designed to ensure that digital entities comply with local laws, standards, and regulations, contributing to a regulated and secure digital market environment.

The DPA team currently distinguishes between the following registration and licensing policy instruments:

- Operational license requirement: Rules for firms to acquire a licence before engaging in certain types of digital businesses. *Example: France and Italy require crypto issuers to obtain a license before operating.*
- Business registration requirement: Rules requiring companies engaging in specific digital activities to register their business. *Example: India requires data processing entities to register their operations.*
- Authorisation of goods or services: Rules demanding government approval for specific digital goods or services before they can be offered to the public. *Example: El Salvador accepts cryptocurrencies as legal tender following official authorisation.*
- Prohibition of goods and services: Rules that explicitly prohibit specific digital goods or services in a market. *Example: Montana Act prohibiting the operation of TikTok and its availability in app stores in the state.*
- Authorisation, registration and licensing, nes: Unspecified rules regarding authorisation, registration, or licensing for the digital economy.

Consumer protection

The consumer protection policy area in the digital economy encompasses regulations aimed at **safeguarding consumer interests**, ensuring fair treatment, and protecting them from potential harms associated with digital products and services. This area focuses on promoting transparency, safety, and fairness in the digital marketplace.

The DPA team currently distinguishes between the following consumer protection policy instruments:

- Fair marketing and advertising practices: Rules requiring digital marketing and advertising to be transparent, truthful, and non-deceptive. *Example: The EU Digital Services Act prohibits dark patterns, which are deceptive designs that mislead consumers into making unintended decisions.*
- User/subject right: Rules upholding the rights of users interacting with digital systems and applications that are unrelated to privacy and expression. *Example: The Chinese regulation of recommendation algorithms grants users several rights, including to be informed of the deployment of recommendation algorithms and their decision processes.*
- Quality of service requirement: Rules requiring digital goods and services to meet safety and quality benchmarks. *Example: South Korea requires internet service providers to maintain stable and high-quality internet services.*
- Age verification requirement: Rules mandating the verification of users' age or the restriction of access to digital services for users under a specific age, often to protect minors. *Example: Utah's amendments to the social media regulations require providers to verify users' age and implement restrictions on the content they view.*
- User identification requirement: Rules requiring firms to identify individuals accessing their service. *Example: The EU regulation on information accompanying transfers of funds mandates crypto-asset service providers to verify information for transfers over EUR 1000 and conduct checks on high-risk entities to prevent money laundering or criminal activities.*
- Non-discrimination requirement: Rules prohibiting discrimination in digital services. *Example: The Chinese generative AI regulation requires providers to effective measures to prevent discrimination due to faith and age, among others.*
- Consumer protection authority governance: Rules changing the powers granted to consumer protection authorities. *Example: The UK Digital Markets, Competition, and Consumers Bill grants the CMA new powers to investigate and enforce consumer protection laws, including the authority to impose monetary penalties for infringements.*
- Consumer protection, nes: Unspecified consumer protection rules that affect the digital economy.

Design and testing standards

The design and testing standards policy area encompasses regulations that ensure digital systems, particularly those incorporating AI and advanced technologies, are **designed and tested to meet specific standards** of performance, safety, interoperability, and user rights. These standards are crucial for ensuring that digital systems function as intended, are free from biases, and respect users' rights.

The DPA team currently distinguishes between the following design and testing policy instruments:

- Design requirement: Rules mandating specific criteria in the design of digital systems. *Example: The EU AI Act requirements for high-risk AI systems regarding the composition of training datasets to ensure diversity and representativeness to mitigate biases and ensure the safety and fairness of AI systems.*
- Testing requirement: Rules to conduct comprehensive testing of digital systems for various aspects like accuracy and bias. *Example: The EU AI Act mandates testing for robustness and bias prior to deploying high-risk AI systems.*
- Performance monitoring requirement: Rules requiring continuous monitoring of digital systems to ensure they perform as expected. *Example: The EU AI Act requires providers of high-risk AI systems to establish and document a post-market monitoring system to ensure that these systems continue to comply with the Act's requirements throughout their lifecycle.*
- Interoperability requirement: Rules mandating firms to ensure their services are interoperable with other systems, promoting compatibility and enhancing competition. *Example: The EU Digital Markets Act (DMA) requires digital "gatekeepers" to make their services interoperable to foster competitive market conditions.*
- Artificial Intelligence authority governance: Rules establishing or changing the jurisdiction of authorities in charge of overseeing providers of Artificial Intelligence. *Example: Spain has established a Spanish Agency for the Supervision of Artificial Intelligence.*
- Design and testing standards, nes: Unspecified design and testing standards that affect the digital economy.

Other operating conditions

The other operating conditions include a range of regulatory instruments that apply to specific **operational aspects** of firms in the digital economy. These policies address the nuances of operating in the digital landscape, focusing on infrastructure use, local operational mandates and similar requirements that do not fall under one of the DPA stand-alone policy areas.

The DPA team currently distinguishes between the following operating condition policy instruments:

- Infrastructure compensation regulation: Rules requiring firms that extensively use digital infrastructure to compensate the providers. *Example: South Korea requires social media platforms to pay more to internet service providers (ISPs) due to the increased traffic they generate.*
- Local operations requirement: Rules obliging firms to maintain a local presence within a jurisdiction to operate, which may include setting up local offices or appointing local employees. *Example: Turkey requires digital payment providers to establish local offices.*
- Mandatory software installation requirement: Rules for firms to install specific software as a condition of providing their service. *Example: Russia requires certain state-approved apps to be pre-installed on smartphones sold in the country.*
- Organisational requirement: Rules requiring firms to implement specific organisational processes and structures, such as quality management systems, defined communication channels, and clear responsibilities towards the public and regulators. *Example: A policy requiring tech companies to establish dedicated channels for regulatory communication.*
- Technology transfer requirement: Rules requiring companies, especially in high-tech industries, to transfer certain technologies as a condition of doing business.
- Other operating condition, nes: Unspecified business operating conditions that affect the digital economy.

Foreign direct investment

The foreign direct investment (FDI) policy area encompasses regulations governing the establishment, ownership, and operations of multinational enterprises (MNEs) within the jurisdiction of a host country. Entry and ownership rules delineate the conditions under which MNEs can enter the market and own assets, often stipulating equity caps or requiring government approval for majority ownership.

The DPA team currently distinguishes between the following foreign direct investment policy instruments:

- MNE: Entry and ownership rule: Pertains to regulations that govern the entry of multinational enterprises into domestic markets and their ownership structures.
- MNE: Financial incentive: Involves financial incentives provided to multinational enterprises to encourage investment or operations in the domestic market.
- MNE: Treatment and operations, nes: Covers a range of treatments and operational conditions for multinational enterprises that are not classified elsewhere.

International trade

The international trade policy area encompasses a spectrum of regulations governing the flow of goods and services across borders.

The DPA team currently distinguishes between the following international trade policy instruments:

- Import licensing requirement: Regulations requiring a license to import certain goods, which can control the volume and type of goods entering a country.
- Import quota: Rules limiting the quantity or value of certain goods that can be imported into a country during a specified time period.
- Import tariff: Taxes imposed on imported goods, which can affect their price and competitiveness in the domestic market.
- Import tariff quota: A hybrid measure that combines a quota and a tariff, where a lower tariff is applied up to a certain import volume, after which a higher tariff is imposed.
- Internal taxation of imports: Taxes applied to imported goods once they have entered the domestic market, separate from customs duties at the border.
- Import ban: Bans certain goods imports to safeguard public health, safety, or local industries.
- Export licensing requirement: Necessitates licenses for exporting specific goods, typically for sensitive or strategic materials.
- Export quota: Limits the quantity of certain goods exported to preserve domestic supply or affect market prices.
- Export tariff: Imposes taxes on exported goods to raise revenue or regulate resource distribution.
- Export tariff quota: Applies a lower export tariff within a set quota, increasing the rate for excess quantities.
- Export subsidy: Government financial support to domestic exporters to enhance global market competitiveness.
- Export ban: Restricts or bans exporting certain goods, usually for national security, environmental, or scarcity concerns.
- Customs duties on electronic transmissions: Rules imposing customs duties on electronic transmissions.
- Border measure, nes: Miscellaneous border measures affecting goods movement across borders.

Public procurement

The public procurement policy area encompasses regulations and practices governing the acquisition of goods and services by governmental entities.

The DPA team currently distinguishes between the following public procurement policy instruments:

- Public procurement blacklisting: Exclusion of certain firms from bidding on public contracts due to previous misconduct.
- Public procurement access: Rules and conditions determining access to public sector contracts.
- Public procurement localisation: Rules requiring public sector entities to procure goods or services from local suppliers, often to support domestic industry.
- Public procurement preference margin: Rules giving preferential treatment in public procurement to certain suppliers, such as small businesses or minority-owned firms.
- Public procurement, nes: Unspecified public procurement rules that affect the digital economy.

Economic activity

The economic activity field in the Digital Policy Alert (DPA) taxonomy identifies the **segments of the digital economy** affected by regulatory changes. This classification helps delineate the scope of digital policies across various sectors. No internationally standardised sectoral nomenclature is available that captures the complexity of the digital economy. Below is the DPA's working version of such a nomenclature. Its fields are subject to change as the need arises to differentiate the different economic activities further.

The DPA team currently distinguishes:

- Cross-cutting: Activities that do not differentiate segments and in principle affect the entire digital economy.
- Digital Payment Provider (including cryptocurrencies): Companies offering digital payment solutions and cryptocurrencies. *Examples: Binance, e-banking services by traditional banks.*
- DLT Provider: Firms providing blockchain technology solutions. *Examples: Ethereum, DAOs.*
- Infrastructure Provider: Cloud Computing, Storage and Databases: Entities offering cloud services, data storage, and database solutions. *Examples: Amazon Web Services, Dropbox.*
- Infrastructure Provider: Internet and Telecom Services: Businesses providing internet and telecommunication services. *Examples: Vodafone, T-Mobile.*
- Infrastructure Provider: Network Hardware and Equipment: Suppliers of hardware and equipment for internet infrastructure. *Examples: Huawei, ZTE, Nokia, Eriksson.*
- Infrastructure Provider: Other: Traditional infrastructure sectors impacted by digital policy.
- Messaging Service Provider: Services for user messaging. *Examples: WhatsApp, Telegram.*
- ML and AI Development Provider: Companies specialising in machine learning and artificial intelligence. *Examples: OpenAI, Anthropic.*
- Online Advertisement Provider: Firms providing digital advertising services. *Examples: Google Ad Services, Facebook Ads.*
- Other Service Provider: Traditional sectors affected by digital policy, such as the financial sector.
- Platform Intermediary: User-generated Content: Platforms for sharing user-generated content. *Examples: Facebook, YouTube, Instagram, TikTok, Reddit.*
- Platform Intermediary: E-commerce: Platforms for online buying and selling. *Examples: Amazon platform, AliExpress, Steam, Facebook Marketplace.*
- Platform Intermediary: Other: Platforms in transport, dating, food, etc. *Examples: Uber, Tinder, Grubhub.*
- Search Service Provider: Web search services. *Example: Google Search.*
- Semiconductors: Companies in semiconductor development and manufacturing. *Examples: NVIDIA, TSMC.*
- Software Provider: App Stores: Application store services. *Examples: Google for Play Store, Apple for App Store.*
- Software Provider: Other: Software providers in various domains. *Examples: Epic Games, Google Chrome, Google Analytics.*
- Streaming Service Provider: Streaming services for various media. *Examples: Spotify, Netflix, Apple Music.*
- Technological Consumer Goods: Producers of consumer technology goods, including IoT devices. *Examples: Mobile phones.*

Event type

Event types within the Digital Policy Alert (DPA) taxonomy categorise the various **legal and regulatory actions** undertaken by different branches of government. These actions can be binding or non-binding and may involve legislative, executive, or judiciary branches.

The binding event types tracked by the DPA team are:

1. Law: A new bill, law, or amendment thereof by the legislature, representing formal and binding legislative actions.
2. Order: A binding pronouncement by the executive branch, often carrying the force of law and requiring compliance.
3. Treaty: A binding agreement between two or more national governments, typically involving the executive branch, establishing commitments at an international level.

The non-binding event types tracked by the DPA team are:

4. Outline: A non-binding guidance by the executive branch that indicates policy interpretation, proposed directions or frameworks for policy but does not have legal force.
6. Inquiry: An exploration into potential policy approaches, which is non-binding and often precedes formal policy proposals or investigations.
7. Declaration: A non-binding statement of position or agreement by a government branch or between national governments, often setting out policy intentions or principles.

In enforcement and litigation, we distinguish:

8. Public Lawsuit: A proceeding in a civil court of law where a government body is a party.
9. Civil Lawsuit: A proceeding in a civil court of law without any government body as a party, still affecting the digital policy landscape through judicial decisions.
10. Investigation: An examination into the private sector by the executive branch, which can be binding if it leads to enforcement actions.

Action type

The action types within the Digital Policy Alert (DPA) taxonomy articulate the **progression of a regulatory change** through various stages, from initial consideration to final enforcement or repeal. These milestones help users understand where a policy is in its overall lifecycle.

The action types reflect the progression of a regulatory change from conception to conclusion:

- Drafting: The creation of initial policy drafts before formal deliberation.
- Announcement: A public statement signalling the start of the policy change process.
- Introduction: The formal commencement of deliberations on a new policy or regulation.
- Consultation Opened: The initiation of a period for public comment on the proposed policy.
- Consultation Closed: The completion of the public consultation period.
- Amendment: Modifications made to current policies or those under consideration.
- Passage: When a proposed law passes one chamber of parliament.
- Rejection: The decision by a deliberative body not to advance a policy further.
- Adoption: The official approval of a policy or regulatory change.
- Signing: The formal ratification of treaties or laws.
- Veto: The disapproval or rejection of a policy by an authoritative body.
- In Force with Grace Period: A law that has been passed but will be implemented after a grace period.
- Implementation: The start of enforcement for a policy or regulatory change.
- Postponement: Delaying the implementation of an adopted policy.
- Termination Announcement: Notification of an upcoming end to an enforced policy.
- Termination: The conclusion of a policy's enforcement period.

For judicial actions, the DPA team further tracks:

- Injunction: A judicial order enforcing or preventing specific actions temporarily.
- Interim Ruling: A preliminary judicial decision or conclusion of an investigation phase.
- Ruling: A court's decision, which may influence policy enforcement or interpretation.
- Closure: The end of a judicial inquiry or investigation with no further action.
- Appeal: The process of challenging a court ruling in a higher court.