

# Messages Swiss IGF 2025

## Session 1: Von der Politik zur Praxis: Kann die KI-Regulierung Wettbewerbsfähigkeit und einen verantwortungsvollen Umgang mit KI in Einklang bringen?

### Key discussions

Die Künstliche Intelligenz hat sich als dauerhafter Bestandteil unserer Gesellschaft etabliert. Eine angemessene Regulierung dieser Technologie scheint angezeigt, sowohl für den öffentlichen als auch für den privaten Sektor um ein gewisses Mass an Rechtssicherheit zu schaffen.

Die aktuelle Situation in der Schweiz ist durch einen hohen Grad an Eigenverantwortung der Unternehmen gekennzeichnet.

Es besteht Bedarf an einer umfassenderen nationalen Vision. Die Schweiz verfügt über das Potenzial, eine Vorreiterrolle in diesem Bereich einzunehmen.

Die Entwicklung vertrauenswürdiger KI-Systeme ist essentiell, um sicherzustellen, dass die Technologie dem Gemeinwohl dient. Die Förderung des Vertrauens liegt in der gemeinsamen Verantwortung von Unternehmen, Regierungen und Regierungsbehörden, welche die verfügbaren Instrumente zur Vertrauensbildung nutzen sollten.

### Key Take Aways

Es sollten praxisorientierte Massnahmen für öffentliche und private Akteure implementiert werden.

Die KI-Regulierung sollte Bestimmungen zur Förderung der KI-Kompetenz enthalten. Neben der Förderung der KI-Kompetenz bei den Bürgerinnen und Bürgern ist auch die Stärkung der Policy-Kompetenz bei Entscheidungsträgern erforderlich. Eine umfassende Weiterbildung aller relevanten Akteure ist notwendig.

## Session 2: Kinder- und Jugendschutz

### Key discussions

Die digitale Welt bietet sowohl Risiken als auch Chancen für Kinder und Jugendliche. Zu den Risiken gehören Profiling, Tracking und Sicherheitslücken, die zu verschiedenen Formen der Gefährdung führen können. Chancen liegen in innovativen Bildungsformen und erweiterten Partizipationsmöglichkeiten. Die digitalen Fussabdrücke von Minderjährigen stellen eine besondere Herausforderung dar, insbesondere wenn Daten durch Erziehungsberechtigte geteilt werden. Das Spannungsverhältnis zwischen Sicherheit und Freiheit erfordert ausgewogene staatliche Massnahmen. Lösungsansätze sollten an der Schnittstelle von Ethik und Recht entwickelt werden. Die Verantwortung liegt nicht allein bei den Erziehungsberechtigten, die teilweise mit den Herausforderungen überfordert sind.

## Key Take Aways

Ein wirksamer Schutz von Kindern und Jugendlichen in der digitalen Welt erfordert die gleichwertige Berücksichtigung dreier Ebenen:

- Die technische Ebene erfordert die Implementierung datenschutzfreundlicher Technikgestaltung. Prinzipien wie Privacy by Default und Privacy by Design müssen frühzeitig, bereits bei der Evaluierung und Beschaffung von Lernapplikationen, berücksichtigt werden.
- Die institutionelle Ebene verlangt, dass Bildungseinrichtungen, digitale Plattformen, Behörden und staatliche Institutionen ihre Prozesse an den spezifischen Schutzbedürfnissen von Kindern und Jugendlichen ausrichten.
- Die gesellschaftliche Ebene erfordert eine umfassende und zielgruppengerechte Sensibilisierung für die Chancen und Risiken der digitalen Welt. Nur digital kompetente Erziehungsberechtigte und Lehrpersonen können Minderjährige adäquat begleiten.

Das Kindeswohl muss als oberste Handlungsmaxime auch im digitalen Raum etabliert werden.

## Session 3: Swiss eID, wie geht es weiter?

### Key discussions

Die technische Umsetzung der eID demonstriert die vorhandenen Kompetenzen in der Schweiz. Dies wirft Fragen bezüglich der strategischen Ausrichtung bei der Nutzung digitaler Infrastrukturen auf.

Wo und in welchem Umfang soll ein Recht auf Offline-Präsenz und auf alternative Zugangsmöglichkeiten bestehen?

### Key Take Aways

Der gewählte partizipative Ansatz bei der Entwicklung der eID hat sich als wertvoll erwiesen und sollte für zukünftige Prozesse als Vorbild dienen. Eine verbesserte Kommunikation über berücksichtigte Aspekte und bestehende Bedürfnisse ist erforderlich, insbesondere aus Bürgerperspektive.

Es gilt, Vertrauen in staatliche digitale Lösungen zu stärken und potenzielle Vorbehalte proaktiv zu adressieren.

Für zukünftige Entwicklungen sollte die Etablierung übergreifender Prinzipien im Vordergrund stehen, um Kohärenz zwischen verschiedenen Gesetzgebungen zu gewährleisten.

## Session 4: Digitale Demokratie – Von E-Voting bis KI-Chatbots

### Key discussions

Auf der Chancen-Seite, können digitale Technologien die Demokratie durch erhöhte Effizienz, Transparenz, Inklusion sowie neue Formen der Partizipation und Deliberation stärken?

Auf der Risiken-Seite, wie soll Herausforderungen um Datenschutz, Privatsphäre, Überwachung, Desinformation, politische Manipulation und Abhängigkeiten von externen Akteuren und Technologien angegangen werden.

Es gilt zu abwägen, welche Gruppen von digitalen Demokratie-Tools profitieren und welche möglicherweise benachteiligt werden. Das Gleichgewicht zwischen Freiheit und Sicherheit muss gewahrt bleiben. Die Frage, ob gesteigerte Effizienz automatisch zu mehr Demokratie führt, bedarf kritischer Betrachtung.

### Key Take Aways

Eine präzise Bedarfsabklärung ist erforderlich: Definition von digitaler Demokratie, Identifikation zu lösender Probleme und Nutzniesser digitaler Lösungen.

Ein robuster rechtlicher Rahmen muss das Recht auf Online- und Offline-Leben schützen, einschliesslich Datenschutz und digitaler Selbstbestimmung.

Digitale Lösungen müssen den schweizerischen Kontext mit Föderalismus und Subsidiarität berücksichtigen, um Vertrauen, Transparenz und Teilhabe zu stärken. Die geopolitische Lage erfordert zusätzliche Aufmerksamkeit für die Resilienz demokratischer Prozesse.

## Session 5: Digitale Souveränität im geopolitischen Tumult: Wie soll sich die Schweiz positionieren?

### Key discussions

Die digitale Souveränität gewinnt aufgrund zweier Entwicklungen an Bedeutung: Veränderungen in der internationalen Ordnung und die durch KI verschärfte globale Wettbewerbssituation.

Die Schweiz hat als digital vernetztes Land erheblich profitiert, jedoch werden digitale Abhängigkeiten zunehmend zu sicherheitspolitischen Herausforderungen.

Die Diskussion umfasste die Auswirkungen geopolitischer Veränderungen auf das Verständnis digitaler Souveränität, die durch KI aufgeworfenen Souveränitätsfragen sowie angemessene Reaktionsstrategien für die Schweiz.

Die in Entwicklung befindliche Strategie für digitale Souveränität der Schweiz basiert auf drei Kernwerten: Subsidiarität, Wirtschaftsfreiheit und Individualverantwortung.

## Key Take Aways

Zeitnahes Handeln ist erforderlich. Konkrete Massnahmen umfassen die Beschaffung alternativer Softwarelösungen für die Verwaltung, die Prüfung von Kooperationsmöglichkeiten mit europäischen Initiativen sowie die Einrichtung einer koordinierenden Stelle für digitale Angelegenheiten auf Bundesebene.

## Session 6: Code, Copyright & Competence: Von der Disruption zur Transformation

### Key discussions

Die Herausforderung besteht darin, einen Rechtsrahmen zu entwickeln, der gleichzeitig Innovation fördert und Kerninteressen schützt (einschliesslich Urheberrechte, Schutz vor Deepfakes und digitale Währungssouveränität).

Es gilt sicherzustellen, dass technologische Entwicklungen der gesamten schweizerischen Wirtschaft zugutekommen. Das bewährte duale Bildungssystem spielt hierbei eine zentrale Rolle.

### Key Take Aways

Regulierung und Innovation sind als komplementäre Elemente zu verstehen. Ein gesamtgesellschaftlicher Ansatz schafft das notwendige Vertrauen und klare Rahmenbedingungen, die Innovation ermöglichen.

Eine dreifache Strategie ist für die wirtschaftliche Positionierung entscheidend:

- Förderung bestehender Innovationskooperationen innerhalb der Schweiz
- Nutzung des dualen Bildungssystems zur breiten Kompetenzentwicklung
- Anwendung des Subsidiaritätsprinzips für nachhaltige KI-Implementierung

Dieser integrative Ansatz ermöglicht umfassende Kompetenzbildung, Vertrauensaufbau, Produktivitätssteigerung und Informationssouveränität.

## Session 7: Daten, Datenschutz und Data Governance

### Key discussions

Der Bundesrat will im kommenden Jahr die Vernehmlassung zu einem Rahmengesetz über die Sekundärnutzung von Daten eröffnen und hat dies zum Schwerpunkt seiner Ziele im Bereich Digitalisierung für das Jahr 2026 erklärt.

Welche Herausforderungen ergeben sich im Hinblick darauf aus sektorieller und übergeordneter horizontaler Sicht für eine solche Rahmengesetzgebung in Bezug auf Data Governance, Datenschutz und weitere Aspekte der wertschöpfenden Datennutzung.

## **Key Take Aways**

Die Diskussion muss auf verschiedenen Ebenen und mit unterschiedlichen Stakeholdern geführt werden, unter Berücksichtigung der Unterschiede der zwischen den Datenkategorien in Bezug auf Grundrechtsschutz, Innovation und Wirtschaftsinteressen.

Es bedarf vertrauenswürdiger Datenräume, um die informationelle Selbstbestimmung praktisch umzusetzen.

Die Sekundärnutzung von Daten soll sowohl dem individuellen wie dem volkswirtschaftlichen Nutzen dienen.

## **Session 8: Die KI-Transformation in der Schweiz: Zugang, Verantwortung und Chancen für alle**

### **Key discussions**

Künstliche Intelligenz (KI) durchdringt zunehmend alle Bereiche unserer Gesellschaft – von Bildung über Arbeitswelt bis hin zu öffentlichen Dienstleistungen. Doch wer stellt sicher, dass alle Menschen in der Schweiz gleichberechtigten Zugang zu den Chancen der KI-Transformation erhalten? Viele Menschen fühlen sich von den technologischen Entwicklungen abgehängt und werden bei der Entwicklung von KI-Systemen nicht miteinbezogen. Im Rahmen der Session wurde diskutiert, wie wir durch «AI Literacy» und inklusive Massnahmen alle Menschen mitnehmen können.

### **Key Take Aways**

Digitale Teilhabe und Inklusion erfordern die Schaffung von Reflexionsräumen auf Augenhöhe unter Berücksichtigung individueller Bedürfnisse.

Ein umfassendes Verständnis potentieller Diskriminierungsrisiken im Umgang mit KI sowie die Förderung verantwortungsvoller Nutzung sind essentiell.

Es braucht auf allen Ebenen verstärkte Bemühungen, die Funktionsweisen, Möglichkeiten und Auswirkungen von KI verständlich zu machen (KI-Kenntnis).

# Session 1: De la politique à la pratique : la réglementation de l'IA peut-elle concilier compétitivité et adoption responsable de l'IA ?

## Discussions clés

L'intelligence artificielle s'est établie comme une composante permanente de notre société. Une réglementation appropriée de cette technologie semble indiquée, tant pour le secteur public que privé, afin de créer un certain niveau de sécurité juridique.

La situation actuelle en Suisse se caractérise par un haut degré de responsabilité propre des entreprises.

Il existe un besoin d'une vision nationale plus complète. La Suisse dispose du potentiel pour assumer un rôle de pionnier dans ce domaine.

Le développement de systèmes d'IA dignes de confiance est essentiel pour garantir que la technologie serve le bien commun. La promotion de la confiance relève de la responsabilité commune des entreprises, des gouvernements et des autorités de régulation, qui devraient utiliser les instruments disponibles pour renforcer la confiance.

## Points clés à retenir

Des mesures orientées vers la pratique devraient être mises en œuvre pour les acteurs publics et privés.

La réglementation de l'IA devrait contenir des dispositions pour promouvoir les compétences en IA. Outre la promotion des compétences en IA chez les citoyens, le renforcement des compétences politiques chez les décideurs est également nécessaire. Une formation continue complète de tous les acteurs concernés est nécessaire.

# Session 2: Protection des enfants et des jeunes

## Discussions clés

Le monde numérique offre à la fois des risques et des opportunités pour les enfants et les jeunes. Les risques comprennent le profilage, le traçage et les failles de sécurité qui peuvent mener à diverses formes de mise en danger. Les opportunités résident dans des formes d'éducation innovantes et des possibilités de participation élargies. Les empreintes numériques des mineurs représentent un défi particulier, notamment lorsque les données sont partagées par les responsables légaux. La tension entre sécurité et liberté exige des mesures gouvernementales équilibrées. Les solutions devraient être développées à l'interface entre l'éthique et le droit. La responsabilité n'incombe pas seulement aux responsables légaux, qui sont en partie dépassés par les défis.

## Points clés à retenir

Une protection efficace des enfants et des jeunes dans le monde numérique nécessite la prise en compte équivalente de trois niveaux:

- Le niveau technique exige la mise en œuvre d'une conception technique respectueuse de la protection des données. Des principes comme Privacy by Default et Privacy by Design doivent être pris en compte dès le début, déjà lors de l'évaluation et de l'acquisition d'applications d'apprentissage.
- Le niveau institutionnel exige que les établissements d'enseignement, les plateformes numériques, les autorités et les institutions étatiques alignent leurs processus sur les besoins de protection spécifiques des enfants et des jeunes.
- Le niveau sociétal exige une sensibilisation complète et adaptée aux groupes cibles sur les opportunités et les risques du monde numérique. Seuls des responsables légaux et des enseignants compétents en matière numérique peuvent accompagner adéquatement les mineurs.

Le bien-être de l'enfant doit être établi comme maxime d'action suprême également dans l'espace numérique.

## **Session 3: Swiss eID, quelle est la prochaine étape ?**

### **Discussions clés**

La mise en œuvre technique de l'eID démontre les compétences existantes en Suisse. Cela soulève des questions concernant l'orientation stratégique dans l'utilisation des infrastructures numériques.

Où et dans quelle mesure devrait exister un droit à la présence hors ligne et aux possibilités d'accès alternatives?

### **Points clés à retenir**

L'approche participative choisie pour le développement de l'eID s'est avérée précieuse et devrait servir de modèle pour les processus futurs. Une meilleure communication sur les aspects pris en compte et les besoins existants est nécessaire, en particulier du point de vue des citoyens.

Il s'agit de renforcer la confiance dans les solutions numériques étatiques et d'aborder proactivement les réserves potentielles.

Pour les développements futurs, l'établissement de principes transversaux devrait être prioritaire afin de garantir la cohérence entre les différentes législations.

## **Session 4: Démocratie numérique – Du vote électronique aux chatbots IA**

### **Discussions clés**

Du côté des opportunités, les technologies numériques peuvent-elles renforcer la démocratie par une efficacité accrue, la transparence, l'inclusion ainsi que de nouvelles formes de participation et de délibération?

Du côté des risques, comment aborder les défis concernant la protection des données, la vie privée, la surveillance, la désinformation, la manipulation politique et les dépendances vis-à-vis d'acteurs et de technologies externes.

Il faut évaluer quels groupes bénéficient des outils de démocratie numérique et lesquels pourraient être désavantagés. L'équilibre entre liberté et sécurité doit être préservé. La question de savoir si une efficacité accrue conduit automatiquement à plus de démocratie nécessite un examen critique.

### **Points clés à retenir**

Une évaluation précise des besoins est nécessaire: définition de la démocratie numérique, identification des problèmes à résoudre et des bénéficiaires des solutions numériques.

Un cadre juridique robuste doit protéger le droit à la vie en ligne et hors ligne, y compris la protection des données et l'autodétermination numérique.

Les solutions numériques doivent tenir compte du contexte suisse avec le fédéralisme et la subsidiarité pour renforcer la confiance, la transparence et la participation. La situation géopolitique nécessite une attention supplémentaire pour la résilience des processus démocratiques.

## **Session 5: La souveraineté numérique dans un contexte géopolitique tumultueux : comment la Suisse doit-elle se positionner ?**

### **Discussions clés**

La souveraineté numérique gagne en importance en raison de deux évolutions: les changements dans l'ordre international et la situation concurrentielle mondiale exacerbée par l'IA.

La Suisse, en tant que pays connecté numériquement, en a considérablement profité, mais les dépendances numériques deviennent de plus en plus des défis de politique de sécurité.

La discussion a porté sur l'impact des changements géopolitiques sur la compréhension de la souveraineté numérique, les questions de souveraineté soulevées par l'IA ainsi que les stratégies de réaction appropriées pour la Suisse.

La stratégie de souveraineté numérique de la Suisse en cours de développement repose sur trois valeurs fondamentales: la subsidiarité, la liberté économique et la responsabilité individuelle.

### **Points clés à retenir**

Une action rapide est nécessaire. Les mesures concrètes comprennent l'acquisition de solutions logicielles alternatives pour l'administration, l'examen des possibilités de coopération avec des initiatives européennes ainsi que la création d'un organe de coordination pour les affaires numériques au niveau fédéral.

## Session 6: Code, copyright et compétence : de la disruption à la transformation

### Discussions clés

Le défi consiste à développer un cadre juridique qui promeut simultanément l'innovation et protège les intérêts fondamentaux (y compris les droits d'auteur, la protection contre les deepfakes et la souveraineté monétaire numérique).

Il faut s'assurer que les développements technologiques profitent à l'ensemble de l'économie suisse. Le système de formation duale éprouvé joue ici un rôle central.

### Points clés à retenir

La réglementation et l'innovation doivent être comprises comme des éléments complémentaires. Une approche sociétale globale crée la confiance nécessaire et des conditions-cadres claires qui permettent l'innovation.

Une triple stratégie est décisive pour le positionnement économique:

- Promotion des coopérations d'innovation existantes au sein de la Suisse
- Utilisation du système de formation duale pour un développement large des compétences
- Application du principe de subsidiarité pour une mise en œuvre durable de l'IA

Cette approche intégrative permet une formation complète des compétences, le renforcement de la confiance, l'augmentation de la productivité et la souveraineté de l'information.

## Session 7: Données, protection des données et gouvernance des données

### Discussions clés

Le Conseil fédéral veut ouvrir l'année prochaine la consultation sur une loi-cadre sur l'utilisation secondaire des données et en a fait la priorité de ses objectifs dans le domaine de la numérisation pour l'année 2026.

Quels défis se posent à cet égard d'un point de vue sectoriel et horizontal global pour une telle législation-cadre en ce qui concerne la gouvernance des données, la protection des données et d'autres aspects de l'utilisation des données créatrice de valeur.

### Points clés à retenir

La discussion doit être menée à différents niveaux et avec différentes parties prenantes, en tenant compte des différences entre les catégories de données en matière de protection des droits fondamentaux, d'innovation et d'intérêts économiques.

Des espaces de données dignes de confiance sont nécessaires pour mettre en œuvre pratiquement l'autodétermination informationnelle.

L'utilisation secondaire des données doit servir à la fois l'utilité individuelle et économique.

## **Session 8: La transformation de l'IA en Suisse : accès, responsabilité et opportunités pour tous**

### **Discussions clés**

L'intelligence artificielle (IA) pénètre de plus en plus tous les domaines de notre société – de l'éducation au monde du travail en passant par les services publics. Mais qui s'assure que toutes les personnes en Suisse bénéficient d'un accès équitable aux opportunités de la transformation de l'IA? De nombreuses personnes se sentent dépassées par les développements technologiques et ne sont pas impliquées dans le développement des systèmes d'IA. Lors de la session, il a été discuté comment nous pouvons inclure toutes les personnes grâce à la "littératie IA" et à des mesures inclusives.

### **Points clés à retenir**

La participation et l'inclusion numériques nécessitent la création d'espaces de réflexion sur un pied d'égalité en tenant compte des besoins individuels.

Une compréhension complète des risques potentiels de discrimination dans l'utilisation de l'IA ainsi que la promotion d'une utilisation responsable sont essentielles.

Des efforts renforcés sont nécessaires à tous les niveaux pour rendre compréhensibles les modes de fonctionnement, les possibilités et les impacts de l'IA (connaissance de l'IA).

# Session 1: From Policy to Practice: Can AI Regulation Align Competitiveness with Responsible AI Adoption?

## Key discussions

Artificial Intelligence has established itself as a permanent component of our society. Appropriate regulation of this technology appears necessary, both for the public and private sectors, to create a certain level of legal certainty.

The current situation in Switzerland is characterized by a high degree of corporate self-responsibility.

There is a need for a more comprehensive national vision. Switzerland has the potential to assume a pioneering role in this field.

The development of trustworthy AI systems is essential to ensure that technology serves the common good. Promoting trust is the shared responsibility of companies, governments, and regulatory authorities, who should use available instruments to build trust.

## Key Take Aways

Practice-oriented measures should be implemented for public and private actors.

AI regulation should contain provisions to promote AI literacy. In addition to promoting AI literacy among citizens, strengthening policy competence among decision-makers is also necessary.

Comprehensive continuing education for all relevant actors is required.

# Session 2: Child and youth protection

## Key discussions

The digital world offers both risks and opportunities for children and young people. Risks include profiling, tracking, and security vulnerabilities that can lead to various forms of endangerment. Opportunities lie in innovative forms of education and expanded participation possibilities. The digital footprints of minors present a particular challenge, especially when data is shared by legal guardians. The tension between security and freedom requires balanced government measures. Solutions should be developed at the interface of ethics and law. The responsibility does not lie solely with legal guardians, who are partly overwhelmed by the challenges.

## Key Take Aways

Effective protection of children and young people in the digital world requires equal consideration of three levels:

- The technical level requires the implementation of privacy-friendly technology design. Principles such as Privacy by Default and Privacy by Design must be considered early on, already during the evaluation and procurement of learning applications.

- The institutional level requires that educational institutions, digital platforms, authorities, and state institutions align their processes with the specific protection needs of children and young people.
- The societal level requires comprehensive and target-group-appropriate awareness of the opportunities and risks of the digital world. Only digitally competent legal guardians and teachers can adequately accompany minors.

The best interests of the child must be established as the supreme principle of action in the digital space as well.

## Session 3: Swiss eID, what's next?

### Key discussions

The technical implementation of the eID demonstrates the existing competencies in Switzerland. This raises questions regarding the strategic direction in the use of digital infrastructures.

Where and to what extent should there be a right to offline presence and alternative access options?

### Key Take Aways

The participatory approach chosen for the development of the eID has proven valuable and should serve as a model for future processes. Improved communication about considered aspects and existing needs is required, especially from the citizens' perspective.

Trust in state digital solutions must be strengthened and potential reservations proactively addressed.

For future developments, the establishment of overarching principles should be prioritized to ensure coherence between different legislations.

## Session 4: Digital Democracy – From E-Voting to AI Chatbots

### Key discussions

On the opportunities side, can digital technologies strengthen democracy through increased efficiency, transparency, inclusion, and new forms of participation and deliberation?

On the risks side, how should challenges regarding data protection, privacy, surveillance, disinformation, political manipulation, and dependencies on external actors and technologies be addressed?

It is necessary to weigh which groups benefit from digital democracy tools and which may be disadvantaged. The balance between freedom and security must be maintained. The question of whether increased efficiency automatically leads to more democracy requires critical examination.

## **Key Take Aways**

Precise needs assessment is required: definition of digital democracy, identification of problems to be solved and beneficiaries of digital solutions.

A robust legal framework must protect the right to online and offline life, including data protection and digital self-determination.

Digital solutions must consider the Swiss context with federalism and subsidiarity to strengthen trust, transparency, and participation. The geopolitical situation requires additional attention to the resilience of democratic processes.

## **Session 5: Digital sovereignty in geopolitical turmoil: How should Switzerland position itself?**

### **Key discussions**

Digital sovereignty is gaining importance due to two developments: changes in the international order and the global competitive situation exacerbated by AI.

Switzerland, as a digitally connected country, has benefited considerably, but digital dependencies are increasingly becoming security policy challenges.

The discussion covered the impact of geopolitical changes on understanding digital sovereignty, sovereignty issues raised by AI, and appropriate response strategies for Switzerland.

Switzerland's developing digital sovereignty strategy is based on three core values: subsidiarity, economic freedom, and individual responsibility.

### **Key Take Aways**

Timely action is required. Concrete measures include procuring alternative software solutions for administration, examining cooperation opportunities with European initiatives, and establishing a coordinating body for digital affairs at the federal level.

## **Session 6: Code, Copyright & Competence: From Disruption to Transformation**

### **Key discussions**

The challenge is to develop a legal framework that simultaneously promotes innovation and protects core interests (including copyrights, protection against deepfakes, and digital monetary sovereignty).

It must be ensured that technological developments benefit the entire Swiss economy. The proven dual education system plays a central role here.

## Key Take Aways

Regulation and innovation are to be understood as complementary elements. A whole-of-society approach creates the necessary trust and clear framework conditions that enable innovation.

A triple strategy is crucial for economic positioning:

- Promotion of existing innovation cooperations within Switzerland
- Use of the dual education system for broad competence development
- Application of the subsidiarity principle for sustainable AI implementation

This integrative approach enables comprehensive competence building, trust building, productivity increase, and information sovereignty.

## Session 7: Data, data protection and data governance

### Key discussions

The Federal Council wants to open consultation on a framework law on the secondary use of data next year and has made this the focus of its goals in the area of digitalization for 2026.

What challenges arise in this regard from a sectoral and overarching horizontal perspective for such framework legislation with respect to data governance, data protection, and other aspects of value-creating data use.

### Key Take Aways

The discussion must be conducted at various levels and with different stakeholders, taking into account the differences between data categories in terms of fundamental rights protection, innovation, and economic interests.

Trustworthy data spaces are needed to practically implement informational self-determination.

Secondary use of data should serve both individual and economic benefit.

## Session 8: AI transformation in Switzerland: access, responsibility and opportunities for all

### Key discussions

Artificial intelligence (AI) increasingly permeates all areas of our society – from education to the workplace to public services. But who ensures that all people in Switzerland have equal access to the opportunities of AI transformation? Many people feel left behind by technological developments and are not involved in the development of AI systems. The session discussed how we can include all people through "AI Literacy" and inclusive measures.

## **Key Take Aways**

Digital participation and inclusion require the creation of reflection spaces at eye level, taking individual needs into account.

A comprehensive understanding of potential discrimination risks in dealing with AI as well as promoting responsible use are essential.

Increased efforts are needed at all levels to make the functioning, possibilities, and impacts of AI understandable (AI knowledge).