



Résumé de la Conférence Cloud et Workplace 2025

Date 19 août 2025

Version 2.0

Auteurs Groupe de travail Cloud Governance et Workplace et intervenants de la conférence

Table des matières

Aperçu des contributions spécialisées	2
Résultats Mentimeter sur le thème des dépendances et de la souveraineté	4
Résultats Mentimeter sur le thème GenKI	10
Feedback des participants	11



La conférence a réuni des représentants de l'administration fédérale, des cantons, d'organisations spécialisées et de prestataires. Elle a porté principalement sur les questions de souveraineté numérique, le développement des solutions cloud et workplace, ainsi que le rôle de l'IA dans le contexte administratif. L'événement était animé par Erich Hofer (CIO de la Direction des travaux publics et des transports du canton de Berne), responsable du groupe de travail Cloud Governance et Workplace.

Aperçu des contributions spécialisées

1. Microsoft Sovereign Cloud et Copilot – Protection des données et gouvernance

Intervenants : Daniel von Büren et Cyril Hollenstein, Microsoft Suisse

- Chez Microsoft, la souveraineté numérique est comprise comme une combinaison de liberté de choix, de contrôle et de performance.
- Les modèles européens de cloud souverain diffèrent en termes de responsabilité, d'emplacement et de degré de contrôle (cloud public, cloud partenaire national, cloud privé). Pour la Suisse, ce sont principalement les modèles publics et privés qui sont à l'avant-plan.
- Copilot dans Microsoft 365 a été présenté comme une interface utilisateur pour l'IA, avec pour priorités :
 - Les données restent sous le contrôle des clients.
 - Pas d'entraînement des modèles avec les données des clients.
 - Respect des limites de données de l'UE et des conditions énoncées dans la déclaration de conditions ANS
 - Utilisation des systèmes de rôles et de conformité existants.

Conclusion : pour les responsables de projet, le type de traitement des données (lieu, cryptage, cadre juridique) est plus important que le type de licence du produit lui-même.

2. Surveillance de la gouvernance du cloud : gestion des changements dans M365

Intervenant : Alexander Hofmann, Laux Lawyers AG

- Les organisations sont confrontées chaque mois à des centaines de mises à jour techniques et juridiques dans l'environnement Microsoft.
- Une surveillance systématique peut réduire considérablement la charge de travail en évaluant, classant et préparant les notifications pour des rôles spécifiques (par exemple, informatique, sécurité, conformité).

Conclusion : la gouvernance du cloud nécessite une surveillance continue et la traduction de changements complexes en informations techniques claires pour la pratique.

3. Cadre juridique pour le cloud et le lieu de travail

Intervenant : Stephan Brunner, Chancellerie fédérale (section Droit)

- Les bases pertinentes sont notamment le traitement des données de commande (art. 9 LPD), la communication à l'étranger (art. 16 ss LPD) et le secret de fonction.
- Les conflits avec les ordres juridiques étrangers (CLOUD Act, FISA, etc.) doivent être pris en compte dans le cadre d'une approche fondée sur les risques.
- Le PFPDT accepte cette approche, pour autant que les risques soient présentés et évalués de manière transparente.

Conclusion : d'un point de vue juridique, le cadre existant est suffisant. Il est essentiel de répartir clairement les responsabilités (responsabilité partagée) et d'atténuer les risques lors de la mise en œuvre.

4. L'open source comme pilier de la souveraineté numérique

Intervenant : Bruno Schöb, Chancellerie fédérale (DTI)

- La souveraineté numérique est renforcée par la diversité et l'indépendance des différents fournisseurs.
- L'art. 9 de l'EM BAG impose la publication du code source développé en interne ou sur mandat.
- Les normes ouvertes et l'open source permettent une meilleure marge de manœuvre en matière de contrôle et d'action.
- Un cadre d'évaluation de la souveraineté numérique a été présenté (perspectives : contrôle technologique, souveraineté des données, capacité de contrôle juridique, résilience, contrôle économique).

Conclusion : l'open source est essentiel, car il crée des possibilités de changement et rend les administrations un peu plus indépendantes des solutions propriétaires.

5. Table ronde sur la souveraineté numérique

Intervenants : Dominic Straub et Nadine Tschichold, ELCA, ainsi que des représentants du groupe de travail ANS

- La souveraineté numérique concerne la technologie, les données, les fournisseurs, les compétences, la conformité et les applications.
- Les risques tels que la dépendance vis-à-vis d'un fournisseur ou l'absence de développement ne peuvent être limités que par des stratégies claires (par exemple, fournisseurs alternatifs, open source, cryptage).
- Un modèle de maturité a été discuté afin d'évaluer systématiquement les progrès et les domaines d'action.

Conclusion : la souveraineté numérique dont il a été question n'est pas un état absolu, mais un équilibre entre les avantages, les coûts, les risques et la faisabilité.

6. Rapport pratique GenAI au sein de la Confédération – Office fédéral de l'environnement (OFEV)

Intervenants : Patrick Koller, OFEV, et Philipp Knecht, AWS Suisse

- L'OFEV développe un agent basé sur l'IA pour aider à traiter les demandes, sur la base d'architectures RAG.
- Défis : intégration des données, multilinguisme, approvisionnement, modèles de coûts.
- Avantages : évaluation plus rapide, réponses plus précises, meilleure utilisation des sources de données existantes.

Conclusion : au niveau administratif, l'IA peut considérablement améliorer l'accessibilité et le traitement de grandes quantités de données. La mise en œuvre conforme à la protection des données reste toutefois déterminante.

7. GenAI dans la pratique administrative – Canton de Saint-Gall

Intervenants : Olaf Sparka (Dép. de l'économie SG), N. Zahn et N. Tschichold (ELCA Advisory)

- Les collaborateurs sont de plus en plus demandeurs d'outils d'IA.
- Un hub GenAI central doit :
 - Assurer la gouvernance (conformité, anonymisation des données)
 - Permettre une mise en œuvre technique flexible (cloud, as-a-service, sur site).
- Il est prévu de mettre en place un produit minimum viable (MVP) sans traitement de données sensibles pour un premier test pratique.

Conclusion : l'introduction de l'IA nécessite des structures de gouvernance claires, des approches itératives (MVP) et un contrôle centralisé.

8. Discours d'ouverture : « L'État numérique n'a pas besoin d'un centre de données, mais de la force de caractère. »

Intervenant : Dominik Steiner, prés. de l'association eGov-Schweiz, parlement cantonal NW

- Plaidoyer en faveur d'une infrastructure numérique fédérale et résiliente en Suisse.
- Six piliers : fédéralisme, résilience, souveraineté des données, innovation, évolutivité, acceptation.
- Vision : autonomie fédérale avec une infrastructure en réseau d'ici 2030.

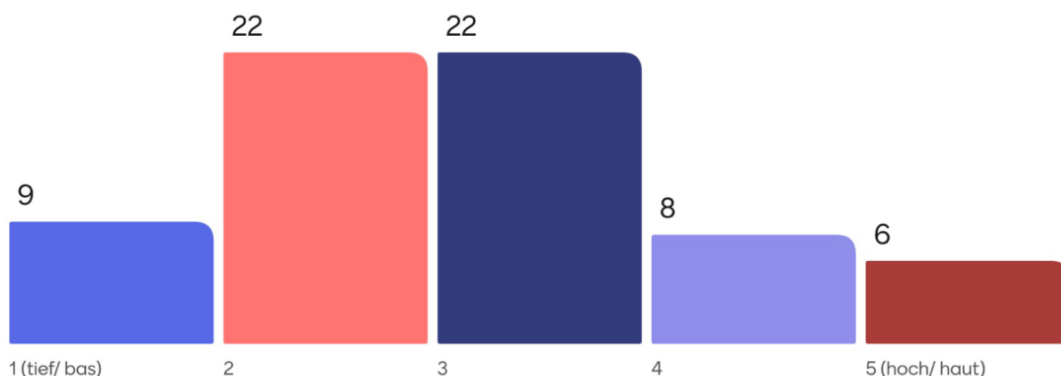
Conclusion : la politique en matière d'infrastructures est aussi une politique de pouvoir. La Suisse devrait mettre à profit ses atouts fédéraux pour asseoir sa souveraineté numérique.

Conclusion et perspectives

La conférence Cloud et Workplace 2025 a montré que l'administration et ses partenaires ne peuvent façonner la transformation du cloud et de l'IA qu'ensemble, dans un cadre juridique, organisationnel et technique clair. Les participants ont apprécié cet événement spécialisé qui fournit des informations pratiques et favorise la discussion. Les prochaines conférences spécialisées se concentreront sur la concrétisation de la gouvernance du cloud, de l'open source et des applications d'IA.

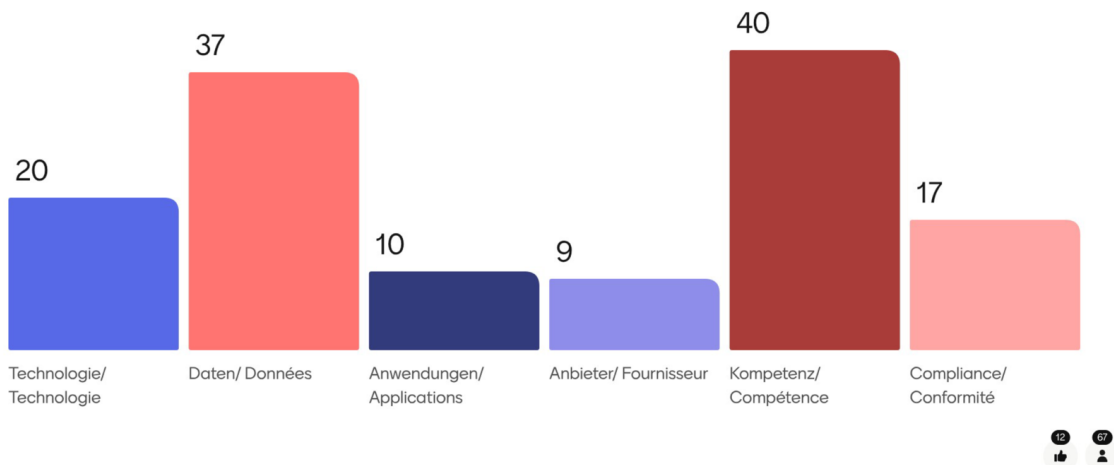
Résultats Mentimeter sur le thème des dépendances et de la souveraineté

Wie beurteilen Sie die digitale Souveränität ihrer Organisation? [Comment évaluez-vous la souveraineté numérique de votre organisation ?](#)

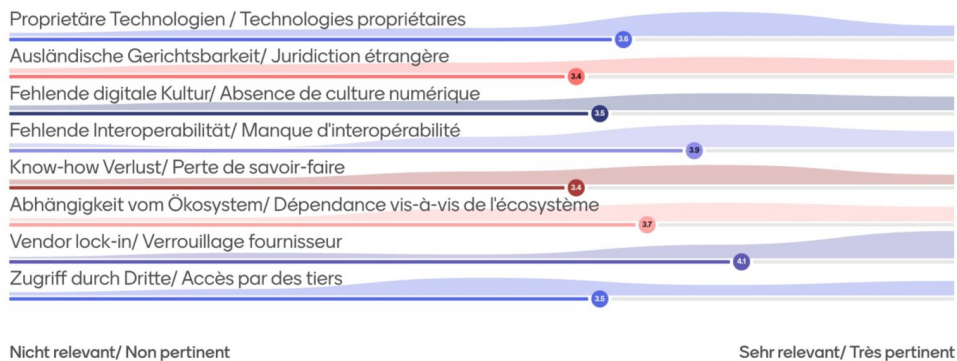


Résumé de la Conférence Cloud et Workplace 2025

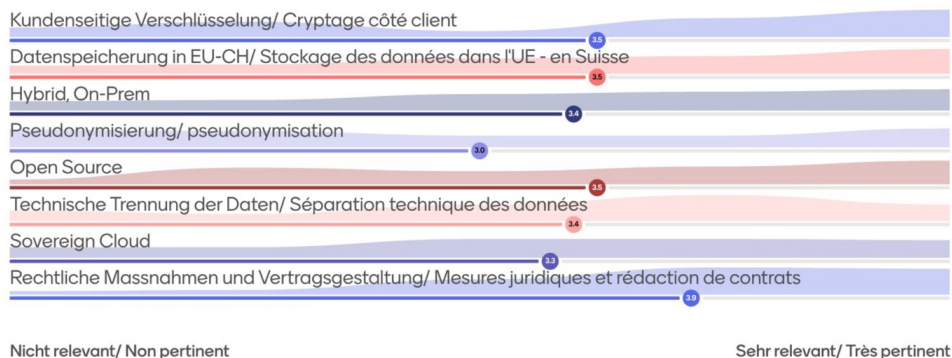
Welche sind die wichtigsten zwei Aspekte für digitale Souveränität? Quels sont les deux aspects les plus importants pour la souveraineté numérique?



Wie relevant sind die folgenden Risiken? Quelle est la pertinence des risques suivants ?

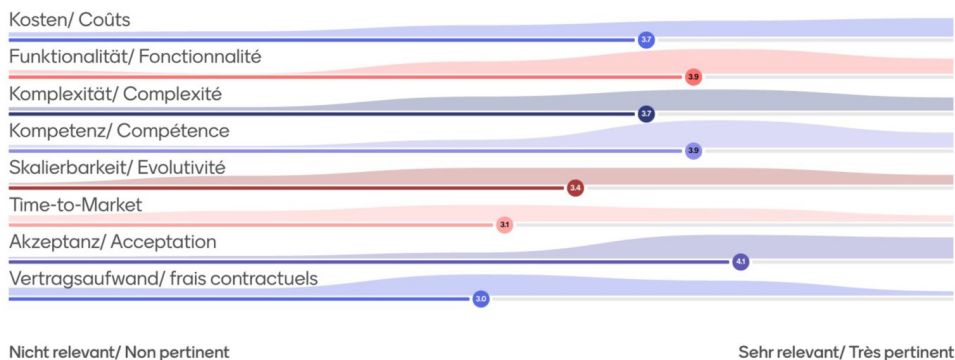


Wie relevant sind die folgenden Massnahmen? Dans quelle proportion les mesures suivantes sont-elles pertinentes ?





Wie wichtig sind die folgenden Herausforderungen für ihre Organisation? Quelle est l'importance des défis suivants pour votre organisation?



Welche Themen wären speziell wichtig wenn eine Studie erarbeitet würde? Quels thèmes seraient particulièrement importants si une étude était élaborée?



Dans quelle mesure ce sujet vous occupera-t-il l'année prochaine ?

Réponses
Moyennement à fortement
Beaucoup, surtout au niveau politique où ce sujet bénéficie actuellement d'un fort élan.
Fortement
Très fortement
Beaucoup, nous devons proposer un catalogue de prestations avec des équivalences gratuites.
Cela dépendra fortement du climat politique. En ce qui concerne M365 en particulier, la situation est actuellement calme chez nous. Dans certaines circonstances, son utilisation pourrait être remise en question de manière plus critique. Cependant, nous n'élaborerons pas de stratégie de sortie l'année prochaine et ne rechercherons pas sérieusement d'alternatives.
Probablement encore plus



très fortement
fort
Fort
Cela dépendra fortement de l'accord auquel parviendront les responsables politiques, ou plutôt de l'influence qu'exerceront les personnalités politiques qui font l'opinion. Cela va de « occupera » à « remplira ».
Nous n'en sommes qu'au tout début du voyage.
En tant que très petit canton, nous ne pouvons participer à aucun POC ni élaborer de concepts à ce sujet. Nous sommes donc très reconnaissants aux groupes de travail DVA pour leur travail et essayons de nous y impliquer davantage.
Pas fort, nous avons d'autres défis à relever.
Encore incertain.
Fort
À mon avis, cela dépend fortement de la situation géopolitique, sur laquelle je ne me risquerai pas à faire de pronostics. D'autre part, l'avenir nous dira comment le « pouvoir des entreprises » sera géré à l'avenir. À cet égard, il s'agira de gérer activement les dépendances. Une première étape dans ce sens consiste à connaître en détail ces dépendances.
Je pense que oui.
Ce sera un sujet important. Malheureusement, il manque une orientation politique sur la manière dont nous devons avancer et sur les ressources qui peuvent être utilisées à cette fin.
Fortement
En cours
Moyen (espérons-le)
Je ne peux pas me prononcer aujourd'hui
Très fort
Il m'occupera de manière très très forte. Vu que l'offre de produits Microsoft on-premise est en train de disparaître. C'est le cas d'Omnisa aussi.
Pas fort
Très fort
Moyen

Quels thèmes seraient particulièrement importants si une étude était élaborée ?

Réponses
Souveraineté technologique (développement, contrôle et disponibilité propres des technologies clés) Souveraineté des données (contrôle des données propres et de leur traitement) Aspects juridiques (réglementation et législation dans l'espace numérique) Aspects économiques (promotion des alternatives européennes, compétitivité) Aspects sociaux (éducation numérique, participation, compétence médiatique) Aspects politiques (sécurité nationale, capacité d'action de l'État)
Prise en compte de toutes les facettes qui ont des conséquences, par exemple les efforts en faveur de l'open source (« à tout prix »), en termes de dépendances, de disponibilité, de qualité de service, etc. Présenter également de manière transparente comment l'open source peut être effectivement « souverain ».
Que signifie une informatique souveraine ? Délimitation des responsabilités : achats sur le marché vs solutions développées en interne.
Open source first - il doit y avoir de bonnes raisons de s'en écarter, en particulier dans le domaine de l'IA. Protection des données Stratégie de sortie
Comment l'utilisation du cloud public dans les autorités critiques (services de renseignement, Fedpol, unités spéciales, armée) influence-t-elle les possibilités de dissimulation, d'anonymisation et de pseudonymisation des identités des utilisateurs, et quels risques cela comporte-t-il pour la protection des forces opérationnelles ?
La liste des équivalences OSS des logiciels payants. Par thématique, avec une base de données alimentée par l'ensemble des membres de l'ANS.
Il existe déjà plusieurs études à ce sujet, nous n'avons actuellement aucun thème particulier à aborder.
À mon avis, les thèmes ont été pris en compte dans l'exemple.
Protection des données
Alternatives au cloud public
Modèles d'exploitation de solutions alternatives (par exemple OpenDesk)
En fait, deux : - Base juridique pour l'utilisation de plateformes hyperscale - OSS dans l'administration - avec pour domaines prioritaires « bureautique », « applications commerciales » et « intégration (en particulier GEVER) » et répercussions sur les finances, la planification et les ressources humaines
Protection des données et autonomie
Considération globale d'un canton quelconque avec plus de 70 applications centrales (Tribuna, Terris, Cari, Gemowin, NEST, Escada, etc. et en plus les anciennes applications fédérales) qui sont étroitement liées aux produits Microsoft. Comment migrer vers les logiciels libres sans perte de stabilité et avec des utilisateurs qui, à 90 %, ne connaissent que M365 ?

La souveraineté peut également être atteinte par le renoncement. Je prends l'exemple du courrier électronique. Si la communication, le traitement des dossiers et la gestion des cas étaient encore plus externalisés vers des systèmes spécialisés. Ou si les systèmes spécialisés n'avaient plus besoin des applications clientes M365, le verrouillage des fournisseurs serait au moins moindre, les fournisseurs pourraient être remplacés sans avoir à passer à des produits open source non gérés. Le cas échéant, l'étude peut également examiner cet aspect de la souveraineté, dans la mesure où nous n'utilisons plus les systèmes Office de manière critique pour notre activité.

Comment éviter une dépendance supplémentaire ?

- Créer une compréhension commune de la souveraineté numérique - Déclarations sur les coûts d'une plus grande indépendance vis-à-vis des hyperscalers (personnel, exploitation, développement) - Risques : aujourd'hui, les risques sont partagés grâce à la coopération avec les hyperscalers - entre les clients - et donc aussi entre les clients - et le fournisseur. Comment cette relation évolue-t-elle lorsque l'on aspire à plus de souveraineté ?

Coopération (il est inutile que chacun réinvente la roue) Culture de l'erreur (tout ne fonctionne pas toujours comme prévu dès le départ) Échange

Comment mesurer la souveraineté ? Définition uniforme de la souveraineté numérique. Quelles mesures seraient judicieuses pour l'administration publique ? Quel niveau doit ou peut être atteint ? Quelles directives devraient émaner du monde politique ? Quelles questions se posent ?

Terminologie, vue d'ensemble des aspects concernés, base juridique et aspects juridiques, approches pour l'opérationnalisation

Qualité, faisabilité, coûts du concept de migration (vers un autre fournisseur) et du concept de sortie (sortie du cloud). Concept et mise en œuvre de la sauvegarde (en particulier type de stockage indépendant du fournisseur (données) et emplacement de stockage indépendant du fournisseur). Défi de la gestion des clés

Dépendances, risques, coûts

Sécurité et protection des données, intelligence artificielle et dépendance vis-à-vis des groupes technologiques mondiaux, cybersécurité et résilience

- Méthodologie d'évaluation de la souveraineté numérique d'une institution (cadre et critères d'évaluation et de dérivation des bases décisionnelles, ainsi que champs d'action et mesures)

Il faudrait étudier formellement les offres de service des sociétés qui proposent des solutions open source « as a service ». Par exemple Infomaniak. Les études actuelles ne sont que des aperçus abstraits. Il faudrait mener des études plus approfondies et des projets pilotes. Il faut les comprendre de manière objective afin de pouvoir les comparer avec les besoins et non avec les offres GAFAM.

Il s'agit avant tout de clarifier les rôles des différents niveaux fédéraux. La souveraineté numérique ne peut être initiée par les collectivités publiques et les cantons à partir de la base (même si de nombreux politiciens locaux sont de cet avis). La Confédération doit être mise à contribution le plus rapidement possible.

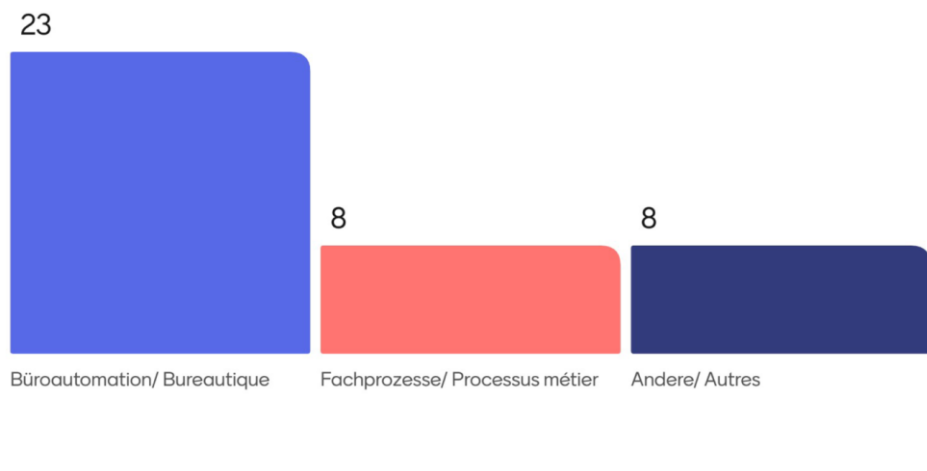
Initiative commune du canton et de la Confédération

Résultats Mentimeter sur le thème GenKI

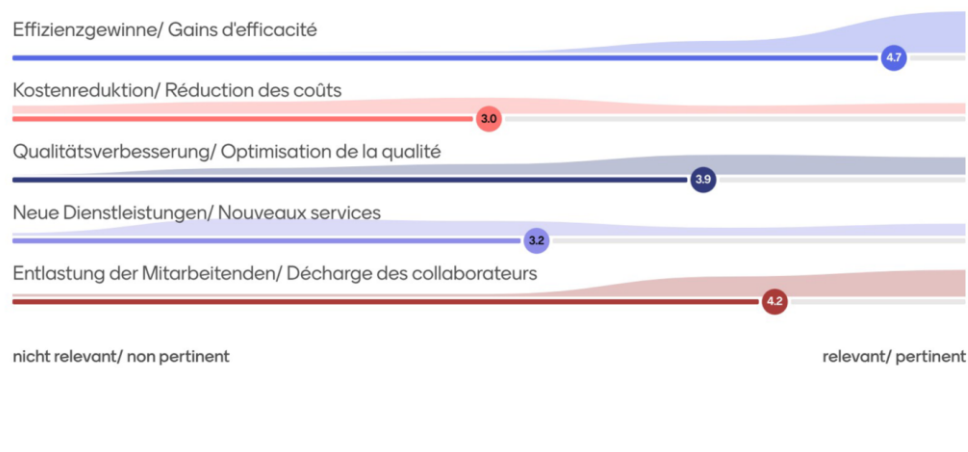
Haben Sie bereits KI-Governance in Ihrer Organisation? [Avez-vous déjà mis en place une gouvernance de l'IA dans votre organisation ?](#)



Wofür wird genKI aktuell in ihrer Organisation primäreingesetzt? [À quoi sert principalement genKI dans votre organisation actuellement?](#)



Was erhoffen Sie vom genKI-Einsatz in ihrer Organisation? [Qu'attendez-vous de l'utilisation de genKI dans votre organisation ?](#)





Was sind die grossen Herausforderungen beim Einsatz von generativer KI? Quels sont les principaux défis liés à l'utilisation de l'IA générative ?

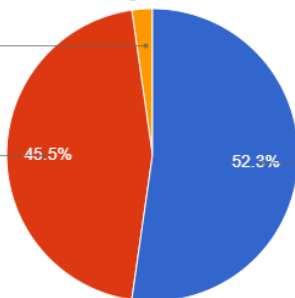


Dans quelle mesure avez-vous été satisfait(e) des thèmes abordés lors de l'événement ?
 Quel a été votre degré de satisfaction quant aux thèmes de l'événement ?

Mässig / suffisant
2.3%

Zufrieden / satisfait
45.5%

Sehr zufrieden / Très satisfait	52,3%
---------------------------------	-------



Option	Pourcentage	Nombre
Très satisfait	52,27	23
Satisfait	45,45	20
Moyen	2,27	1
Insatisfait	0,00	0

Open Source - Souveraineté numérique (BK, CF)

IA pour le lieu de travail (SG)

GenAI à la Confédération (OFEV)