Email Provider Dependencies and Email Security in Municipalities Across Germany, Austria, and Switzerland

Mario Bischof[1⋆], David Huser[2⋆], Alexej Ochsner[3], Ronald Petrlic[4(✉)], and Edy Portmann[1]

[1] Human-IST Institute, University of Fribourg, Fribourg, Switzerland
{mario.bischof, edy.portmann}@unifr.ch
[2] Lucerne University of Applied Sciences and Arts, Lucerne, Switzerland
david.huser@hslu.ch
[3] Technical University of Applied Sciences Ingolstadt, Ingolstadt, Germany
alo0232@thi.de
[4] Nuremberg Institute of Technology, Nuremberg, Germany
ronald.petrlic@th-nuernberg.de

Abstract. Municipal email systems form a critical yet understudied component of public-sector infrastructure, where security requirements intersect with growing dependence on external service providers. We present the first comprehensive, large-scale measurement study of email security and provider dependencies across municipalities in Germany, Austria, and Switzerland, covering more than 15,000 domains.
Our analysis combines DNS-based provider fingerprinting with active security measurements to jointly assess infrastructural centralization and the quality of SPF, DMARC, and DANE deployment. We uncover pronounced cross-country differences, with Germany largely relying on domestic providers, while Austria and Switzerland exhibit strong concentration on US-based cloud platforms. Despite high nominal adoption of SPF, we identify substantial deployment gaps: strict enforcement policies and effective DMARC configurations are rare, and DANE adoption remains negligible. Crucially, provider category predicts the shape of a municipality's authentication posture rather than a scalar security level: US-cloud achieves high rates on strict SPF, whereas domestic providers achieve a roughly twice as large coverage of strict DMARC in every country, and DANE is almost exclusively a domestic phenomenon. Our findings reveal systemic risks arising from both misconfigured authentication and infrastructural concentration, bridging the gap between technical email security research and the emerging discourse on digital sovereignty in European countries.

⋆ both first authors

This is an Accepted Manuscript version of the following work: Computer Security. ESORICS 2026 International Workshops, 2026, Springer Nature Switzerland. This version of the manuscript has been accepted for publication, after final editorial and peer review is complete, but is not the Version of Record and does not reflect post-acceptance improvements (such as copyediting or typesetting), or any corrections. The final authenticated version will be available online at Springer (DOI pending). Use of this Accepted Manuscript version is subject to the publisher's Accepted Manuscript terms of use: https://www.springernature.com/gp/open-research/policies/accepted-manuscript-terms.

Keywords: Email Security · Provider Classification · Digital Sovereignty

1 Introduction

Email communication constitutes a critical component of administrative operations within cities and municipalities. It serves not only as an internal channel for coordination between departments, but also as a primary medium for communication with other public authorities, private organizations, and citizens. These interactions cover a wide range of use cases, including routine service delivery such as handling citizen inquiries, permits, and billing, as well as legally relevant exchanges such as administrative decisions and document submissions. In addition, email is used for disseminating public information, coordinating inter-agency workflows, and supporting crisis response during emergencies. As a result, municipal email systems routinely process sensitive and personally identifiable information and form a core part of public-sector digital infrastructure.

This central role makes email communication a high-value target for attacks. In particular, failures to ensure authenticity and integrity enable spoofing and phishing attacks, where adversaries impersonate municipal domains to deceive recipients. Such attacks can have severe consequences, ranging from financial fraud and data breaches to erosion of public trust in government institutions. The deployment of standardized authentication mechanisms—such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), complemented by Domain-based Message Authentication, Reporting and Conformance (DMARC)—is therefore essential. Without these mechanisms, recipients—including citizens, businesses, and other authorities—cannot reliably verify that an email actually originates from the claimed municipal domain. In practice, this undermines trust in digital communication and weakens the security of administrative processes.

At the same time, the infrastructure underlying municipal email communication is increasingly outsourced to external service providers, often large cloud platforms. While such outsourcing can provide operational benefits, including scalability and professionalized security management, it also introduces structural risks. In particular, strong centralization of municipal hosting can lead to single points of failure and attack. A compromise, misconfiguration, or outage at a dominant provider can simultaneously affect a large number of municipalities, potentially disrupting public services at scale. Moreover, such dependencies raise broader concerns regarding control over data, exposure to foreign jurisdictions, and long-term vendor lock-in. These concerns are commonly framed under the notion of digital sovereignty, which emphasizes the ability of public institutions to retain meaningful control over their digital infrastructure and data.

In this paper, we investigate the state of email security and digital sovereignty in European municipalities through a large-scale empirical analysis. Focusing on three countries: Austria, Germany, and Switzerland (collectively known as DACH), with a population of more than 100 million people, we analyze more than 15,000 municipal email domains and their corresponding mail server infras-

tructures. Our study examines (i) hosting patterns and dependencies on external providers, including the degree of centralization, (ii) the deployment of key email security mechanisms such as SPF, DMARC, and DANE, and (iii) the extent to which established governmental recommendations are implemented in practice. By combining measurements of technical security controls with an assessment of infrastructural dependencies, we provide a comprehensive view of how municipalities balance security requirements with broader concerns of digital sovereignty.

Our findings contribute to the understanding of real-world deployment gaps, structural risks, and policy implications in the public sector's email ecosystem. In particular, they shed light on the security implications of centralized infrastructures and the risks arising from insufficient authentication, thereby informing ongoing debates on secure and sovereign digital infrastructures in Europe.

1.1 Contributions

This paper presents the first large-scale empirical study of email security and infrastructural dependencies in municipal administrations across Germany, Austria and Switzerland. Our main contributions are:

- **Cross-country measurement of municipal email infrastructures:** We perform a systematic analysis of thousands of municipal domains across three countries, providing the first comparative view of how municipal email services are hosted. Despite the strongly federal organization of these countries, we observe clear regional clustering and recurring provider choices, revealing implicit centralization patterns in public-sector email infrastructures.
- **Linking provider choice to security posture:** We correlate SPF, DMARC and DANE deployment with the underlying hosting provider, finding that provider choice predicts the *shape* of security posture: US-cloud excels only on strict SPF, while domestic operators lead on strict DMARC with roughly two times higher adoption and carry the vast majority of DANE support.
- **Our pipeline, datasets and maps are public and open-source**[1] to facilitate the reproducibility of our research results, make our instruments available to the community and support future work.

The remainder of this paper is structured as follows. In Sect. 2 we give a background on email security and present related work in Sect. 3. In Sect. 4 we present the methodology of our investigation, before we present the results in terms of provider choice and security mechanisms in Sect. 5. In Sect. 6 we discuss our findings before we conclude the paper in Sect. 7.

2 Background

Email is a fundamental communication technology in municipal administration. It is used for internal coordination, inter-agency exchange, and direct interaction with citizens, often involving sensitive or personally identifiable information. As

[1] `https://github.com/mxmap/secassure2026/` (code + datasets), `https://secassure2026.mxmap-project.org/` (interactive maps)

a result, municipal email systems must ensure both confidentiality and authenticity. These requirements arise not only from technical threat models—such as spoofing, phishing, and interception—but also from legal obligations governing the processing of personal data and the operation of public administration.

2.1 Technical Standards for Email Security

The *Simple Mail Transfer Protocol* (SMTP), which underlies email delivery, was not originally designed with strong security guarantees. Modern email security therefore relies on a layered set of extensions and complementary protocols. Transport-level confidentiality is typically achieved through TLS between mail servers. However, standard opportunistic TLS is vulnerable to active attacks. Mechanisms such as *DNS-based Authentication of Named Entities* (DANE), which leverages DNSSEC to bind certificates to domain names, strengthen transport security by reducing reliance on the global certificate authority ecosystem and preventing certain classes of man-in-the-middle attacks. Sender authentication and anti-spoofing are addressed through *Sender Policy Framework* (SPF), *DomainKeys Identified Mail* (DKIM), and *Domain-based Message Authentication, Reporting, and Conformance* (DMARC). SPF allows receivers to verify whether a sending server is authorized for a domain, DKIM provides cryptographic message signing at the domain level, and DMARC enforces alignment and defines receiver policies and reporting mechanisms. These standards are widely recognized as the current baseline for protecting against domain impersonation and phishing attacks. Importantly, these mechanisms address different threat vectors and must be deployed jointly. A secure municipal email infrastructure therefore requires a combination of transport security (TLS, ideally hardened via DANE) and domain authentication (SPF, DKIM, DMARC). In practice, deployment gaps are common and partial adoption can leave systems vulnerable despite the presence of individual controls.

2.2 Legal and Regulatory Frameworks

Across all three countries, municipalities are legally obligated to ensure secure data processing, but the choice of specific technical measures is left open and assessed against the state of the art.

In **Germany** and **Austria**, this obligation derives from Article 32 GDPR, which requires "appropriate technical and organizational measures" proportionate to risk. Germany's BSI provides concrete benchmarks through technical guidelines on secure email transport (*TR-03108*) and email authentication (*TR-03182*), as well as the *IT-Grundschutz* framework with dedicated profiles for municipal administration. Although formally binding only for federal authorities, BSI standards are widely referenced in state-level regulations and procurement, making them de facto requirements. However, BSI's formal enforcement powers extend chiefly to operators of critical infrastructure; municipalities typically fall outside this scope and, therefore, rely on BSI guidance as a benchmark rather than as directly enforceable obligations. Austria relies on the *E-Government Act* and its NIS2 implementation; municipalities are not uniformly classified

as essential-service operators but are often indirectly affected through shared infrastructure dependencies.

Switzerland has a similar position outside the EU. The revised *Federal Act on Data Protection* (FADP), in effect since September 2023, imposes analogous requirements [32]. The NCSC documents a sharply rising phishing landscape [18, 20], and since April 2025 critical infrastructure operators must report cyber incidents [19]. SWITCH promotes DNSSEC, DANE, and DMARC adoption through its DNS Resilience Programme [28]. In November 2025, privatim—the conference of Swiss cantonal data protection commissioners—declared outsourcing sensitive personal data to international cloud providers generally inadmissible [22].

In this context, the deployment of SPF, DKIM, DMARC, and DANE serves as a practical indicator of whether municipalities meet their legal obligations, while the choice of hosting provider raises additional compliance questions.

2.3 Digital Sovereignty in Municipal Email Infrastructures

Beyond technical security and legal compliance, the concept of digital sovereignty introduces an additional dimension to the analysis of municipal email systems. In European policy discourse, digital sovereignty refers to the ability of public institutions to maintain control over their digital infrastructure, data, and technological dependencies. In the context of municipal email, digital sovereignty manifests itself in several interrelated challenges. First, there is the question of infrastructure control. Many municipalities rely on external service providers—often large, non-European cloud providers—for email hosting. Although such providers may offer high levels of operational security, they can limit the municipality's ability to independently configure, audit, or extend security mechanisms. Second, there is the issue of jurisdiction and data access. When email services are hosted by providers subject to foreign legal regimes, questions arise regarding government access, data transfers, and compliance with domestic and European data protection requirements. Even where legal transfer mechanisms exist, such as adequacy decisions, concerns about effective control and enforceability remain. Third, there is a dependency and lock-in dimension. The consolidation of municipal email services among a small number of providers can create structural dependencies that are difficult to reverse. This affects not only security decisions but also broader aspects of digital administration, including interoperability, long-term costs, and strategic autonomy. Finally, there is a potential tension between security and sovereignty. Centralized providers may achieve higher baseline security through economies of scale, standardized configurations, and dedicated security teams. However, this may come at the cost of reduced transparency and diminished local control. In contrast, self- or nationally-hosted solutions may enhance sovereignty but require sufficient resources and expertise to maintain a comparable level. Together, these factors illustrate that municipal email systems are at the intersection of technical security, legal compliance, and strategic autonomy. Assessing the deployment of email security mechanisms alongside hosting dependencies therefore provides valuable insight into how municipalities in Germany, Austria, and Switzerland navigate the trade-offs between security and digital sovereignty.

3 Related Work

Previous work has extensively investigated the real-world deployment of email authentication and transport security mechanisms such as SPF, DKIM, DMARC, and DANE. Large-scale measurement studies consistently show that, while adoption has increased over time, deployment remains incomplete and frequently suffers from configuration and operational flaws. Tatang et al. demonstrate the evolution of SPF, DKIM, and DMARC and identify persistent misconfigurations despite increasing adoption [31]. Lee et al. show that DANE adoption remains limited and often misconfigured [13]. Lange et al. confirmed this finding in a more recent study. They investigated 4,000 German health institutions and found that old SSL/TLS versions can still be found in practice and that the implementation of DANE is stuck at around 1% even in this highly sensitive health domain. The authors conclude that thus, German health institutions are not allowed to exchange sensitive health data by email (without additional measures) according to the requirements set by the data protection authorities [12]. A comprehensive ecosystem view by Blechschmidt et al. further reveals inconsistent enforcement and missing validation across the email ecosystem [1].

More recent work confirms that these problems persist and remain relevant today. Hureau et al. show that DMARC deployment is still hindered by misunderstandings and operational errors, and uncover new risks such as data leakage through misconfigured reporting addresses [10]. Similarly, Czybik et al. provide one of the largest recent SPF studies, analyzing 12 million domains and showing that although 56.5 % deploy SPF, a substantial fraction contain errors or overly permissive policies that weaken protection [4]. These findings reinforce that even widely adopted mechanisms are often deployed insecurely in practice.

The existing literature documents that hyperscaler email infrastructure does not uniformly deliver stronger authentication properties. Hu and Wang show that hyperscaler receivers (Gmail, Outlook) routinely fail to enforce published SPF/DMARC policies [9]. Liu et al. measured 16 leading providers and showed that email forwarding at Gmail, Microsoft Outlook, and others systematically breaks SPF/DMARC alignment, permitting spoofed messages to reach recipient inboxes despite authentication [14]. Hager et al. pointed out in a recent study from 2026 that Microsoft faces severe problems with its DNS infrastructure—leading to an almost 10 % rate of DKIM temp errors for emails sent to Exchange Online accounts [8].

Recent research also shows that the threat landscape is evolving beyond protocol weaknesses. Advances in machine learning and large language models (LLMs) have significantly increased the sophistication of phishing attacks. Mahendru et al. show that modern NLP models can achieve high accuracy in detecting phishing emails, but also highlight the increasing realism of attacks [16]. Qi et al. demonstrate that LLMs can generate highly convincing spearphishing emails that evade both automated and human detection [23]. These developments further increase the importance of robust and correctly deployed authentication mechanisms, as content-based defenses alone become less reliable.

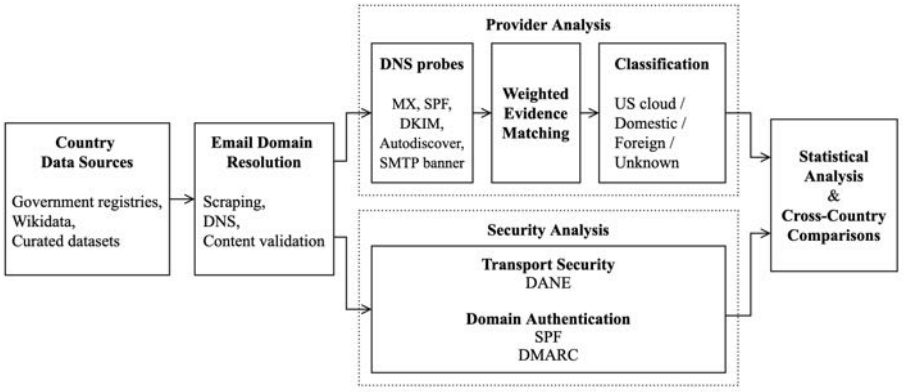

Fig. 1: Methodology overview.

A recent large-scale assessment of government web platforms in all 193 UN member states reveals persistent gaps in secure protocol adoption [24], but does not cover email infrastructure or municipal-level granularity.

In parallel, a growing body of literature addresses the concept of digital sovereignty, particularly in the European context. This work is largely conceptual and policy-oriented. Tan et al. define digital sovereignty as control over digital assets and infrastructures [30], while Fratini et al. analyze different sovereignty models and their implications [7]. Martínez-Ramil et al. conceptualize European digital sovereignty as a multidimensional construct spanning strategic autonomy and governance capacity [17]. Falkner et al. show that EU policymaking increasingly emphasizes control over digital infrastructures, though implementation often lags behind rhetoric [5]. Foundational work by Floridi and Roberts et al. further links digital sovereignty to autonomy, dependency, and governance of critical infrastructures [6, 25].

Taken together, prior work highlights two largely separate research streams. Empirical studies show that email-security mechanisms are inconsistently deployed and often ineffective in practice, while digital-sovereignty research emphasizes control over infrastructure without grounding these concerns in technical measurements. Our work bridges this gap by jointly analyzing email-security deployment and hosting dependencies in municipal infrastructures, thereby linking technical security properties with questions of infrastructural control.

4 Methodology

Our investigation comprises three stages: (1) resolving each municipality's authoritative email domain via multi-source collection and web scraping, (2) classifying the provider through DNS fingerprinting, and (3) analyzing the infrastructure's security. The complete pipeline is visualized in Figure 1.

4.1 Email Domain Resolution

Each municipality's email domain is determined by a seven-phase pipeline, with data sources, configuration parameters, and domain guessing patterns adapted per country. As no official municipal email datasets exist, candidates are sourced from public repositories and selected via the heuristics below.

Phase 1: Candidate Collection. Candidate domains are drawn from multiple sources (Sect. 4.4). If none emerge, we expand the municipality name into country-specific slug variants and apply a template list (e.g., `stadt-{slug}.de`, `gemeinde-{slug}.ch`); Austria always adds `.gv.at`.

Phase 2–4: Validation. Three filters eliminate non-viable candidates: (i) DNS A/AAAA lookups discard unresolvable domains via a multi-resolver fallback chain (system, Quad9, Cloudflare); (ii) HTTP HEAD requests verify accessibility and follow redirects; (iii) a content classifier flags parked domains and checks relevance through German, French, and Italian keywords.

Phase 5: Email Extraction. Accessible, non-parked candidates are scraped exhaustively: the scraper fetches the homepage, discovers contact subpages via static path lists (e.g., `/kontakt`, `/impressum`) and dynamic link extraction, then applies 10 deobfuscation handlers—covering TYPO3 `linkTo_UnCryptMailto` (Caesar), Cloudflare Email Protection (XOR), JavaScript concatenation, Base64 attributes, Joomla SP Page Builder forms, ROT13, and `(at)`/`[at]` substitutions, among others. Pages returning no emails are retried with headless Chromium (Playwright) for JavaScript-rendered content.

Phase 6: MX Validation. All candidate and scraped domains are checked for MX records; those without valid records are excluded.

Phase 7: Decision. The pipeline selects each municipality's domain via a five-tier priority cascade: (1) manual overrides; (2) scraped domains with MX records, filtered by a frequency-based blocklist (domains appearing in $> 0.5\%$ of municipalities) and ranked by name relevance; (3) static-source domains with MX; (4) guessed domains with MX; (5) no domain found. Within each tier, government TLDs (e.g., `.gv.at`) and name-matching domains are preferred. Each result receives a confidence level (high, medium, low, none) based on tier and corroborating evidence.

4.2 Email Provider Classification

We classify each municipality's email provider using DNS fingerprinting that aggregates evidence from 11 probes per domain. Previous work used 4 signals (MX, SMTP banner/EHLO, TLS) for larger-scale domains [15]; to our knowledge, no prior study has applied this to municipal email domains.

DNS Probes. For each domain, the probes in Table 1 execute concurrently.

Provider Signatures. We maintain fingerprint signatures for 3 US-based cloud providers: Microsoft 365, Google Workspace, and Amazon SES, specifying expected patterns across all probes using case-insensitive substring matching.

Table 1: Overview of the 11 probes

Probe	Core Mechanism
MX	Match hostnames against provider signatures.
SPF	Match `include:` directives against provider domains.
DKIM	Resolve CNAMEs for provider-specific selectors.
DMARC	Match `_dmarc` TXT records against reporting addresses.
Autodiscover	Query CNAME/SRV records for Exchange endpoints.
CNAME chain	Follow MX chains (up to 10 hops) to detect infrastructure.
SMTP banner	Port 25: Match 220 banner and EHLO response.
Tenant	Query Microsoft 365 `GetUserRealm` for active tenants.
ASN	Resolve MX IPs to ASNs via Team Cymru [29]; classify by country.
TXT verify	Check for provider-specific tokens (e.g., `MS=ms`).
SPF IP	Map `ip4:`/`a:` entries to ASNs; classify by country.

Gateway (GW) Detection. Before aggregation, MX hostnames are checked against 22 known security gateways (e.g., SEPPmail, Barracuda, Hornetsecurity, Proofpoint). A detection indicates that mail is routed through a filtering proxy, which influences signal weighting during aggregation.

Evidence Aggregation. Evidence is deduplicated by provider/signal kind and the provider with the highest primary signal weights sum wins. Primary signals are MX (0.20), SPF (0.20), DKIM (0.15), and Autodiscover (0.08), summing to 0.63. When a GW is detected, DKIM receives a bonus of 0.06, as DKIM signatures pass through GW's whereas MX/SPF may point to the intermediary.

Confidence Scoring. Confidence (0–100%) is determined by matching the winner's signals against 16 predefined combinations: 3 corroborating primary signals yield 90–95%, 2 yield 60–90%, and 1 yields 50–80%. Any signal not required by the matched rule adds 2 percentage points, capped at 100%. The Microsoft tenant probe boosts confidence but cannot determine the winner independently.

Geolocation Fallback. If no cloud provider signature matches, we fallback to IP-based geolocation: if the MX host's ASN is registered in the target country, the domain is classified as *domestic*; otherwise as *foreign*. These classifications receive lower confidence (0–80%) reflecting coarser granularity. Domains where a GW blocks all primary signals are classified as *unknown*.

Classification Rules. The provider classification follows the rule-based approach shown in Table 2. The algorithm predicts the email provider by evaluating the collected signals as previously explained. As a final result, it categorizes it into one of the following categories: *us cloud*, *domestic*, *foreign* or *unknown*. Since DNS records can be outdated, mid-migration, or ancillary services (e.g. an SPF include for MS Teams), predictions have a confidence level.

Validation. We sent bounce probes to provably non-existent addresses at a stratified sample of 398 municipalities. Parsing DNS headers of the resulting non-delivery reports (NDRs, 84.7% response rate) yields at least 97.2% agree-

Table 2: Classification logic rules

Category	Rule Name	MX	SPF	DKIM	GW	Conf.
us cloud	mx_spf	x	x			90%
	mx_only	x				80%
	spf_gw		x		x	70%
	dkim_gw			x	x	65%
	dkim_spf		x	x		60%
	spf_only		x			50%
	fallback					40%
domestic	dom_mx_spf	x	x			80%
	dom_mx_only	x				70%
	dom_secondary					20%
	dom_none					0%
foreign	frg_mx_spf	x	x			60%
	frg_mx_only	x				50%
	frg_secondary					10%
	frg_none					0%
unknown	gw_no_primary				x	

ment with predictions and a weighted F1 of 0.98 for Microsoft, self-hosted, and Google (n=317, 95% CI ±5.4 pp), consistent with the 97% reported by Liu et al. for a comparable DNS-based classifier [15]. Most remaining disagreements trace to security gateways that absorbed the probe before it reached the predicted provider, leaving those cases inconclusive. Neither method identifies the back-end provider when an on-premise gateway rejects first: both see the gateway and agree on *self-hosted*, creating a shared blind spot. Among self-hosted domains, 174 (1.5%) carry two or more primary Microsoft 365 email indicators (SPF `include`, DKIM selectors) despite domestic MX, suggesting cloud back-ends behind on-premises gateways that neither method can confirm. This bias conservatively understates cloud adoption.

4.3 Security Posture Analysis

The email domains collected in 4.1 are passed through security checks for DANE, SPF, and DMARC. The scanning tool consists of two modules: a *scanner* that resolves MX records and IP addresses, then runs DANE (via `gotls`) and DSS[2] (SPF/DMARC) probes against each domain; and an *evaluator* normalizing the results into a structured JSON database for analysis. It was deployed on a virtual server with outbound port 25 open required for SMTP STARTTLS probes.

We adopt strict enforcement thresholds: only SPF records with an `-all` (fail) policy and DMARC policies set to `reject` are classified as "good", since weaker settings still permit spoofed emails to be accepted by receivers.

We excluded DKIM in the security evaluation because reliable large-scale measurement is not feasible (however for classifications of known providers it is useful). DKIM relies on domain-specific selectors that are not publicly enumerable and must be known in advance to query the corresponding DNS records.

[2] `https://github.com/globalcyberalliance/domain-security-scanner`

Table 3: Country-level overview of email provider classification

Country	n	MS	GO	AZ	Dom	Frg	Unk	Dom	US	Conf[1]	GW[2]
Germany	11,129	793	8	0	9,647	147	534	86.7%	7.2%	75.7%	5.3%
Austria	2,092	1,401	0	0	604	36	51	28.9%	67.0%	85.2%	36.8%
Switzerl.	2,110	1,099	4	22	878	14	93	41.6%	53.3%	84.9%	9.6%
Total	**15,331**	**3,293**	**12**	**22**	**11,129**	**197**	**678**	**72.6%**	**21.7%**	**78.3%**	**10.2%**

[1] Mean classification confidence; 762 municipalities below 60% overall.
[2] Percentage of municipalities routing email through a known security gateway.

Although some large providers use predictable selector naming schemes, this is not generally the case, making comprehensive and unbiased measurement infeasible without access to actual email traffic. As a result, we focus our analysis on mechanisms that can be consistently and reliably evaluated across all domains.

4.4 Municipality Datasets

Our study covers all DACH-municipalities as of April 2026, totaling 15,331. For **Germany**, the Livenson [11] and B42Labs [3] datasets provide domain mappings for approximately 11,000 municipalities; a CSV-based email list compiled from state statistical offices and municipal websites (7,000 entries) by an author, and Wikidata adds website URLs for approximately 3,000 municipalities. For **Austria**, municipalities are sourced from OpenPLZ API [21] across all nine federate states (Bundesländer); the BRESU dataset [2] provides both website and email domains, and Wikidata supplements website discovery. For **Switzerland**, we access the federal government's BFS API [26], with canton assignments enriched from OpenPLZ API and websites discovered via Wikidata; manual overrides correct 142 known errors. The pipeline ran between April 5 and April 12, 2026.

4.5 Ethical Considerations

All scans are non-intrusive querying public data only such as DNS records, HTTP metadata, and standard SMTP handshakes at low rate limits via public resolvers. Validation used rate-limited bounce probes to non-existent recipients. No human subjects or personally identifiable information was involved.

5 Results

5.1 Provider Analysis

Table 3 displays the summary overview of the detected providers, the average confidence and the share of detected gateways. For a regional breakdown, refer to Table 5 in Appendix B and for color-coded maps to Figure 3 in Appendix A.

Germany Germany stands apart from Austria and Switzerland with largely domestic email infrastructure: 87 % of 11,129 municipalities use domestic providers, while US-cloud accounts for only 7 %—almost entirely Microsoft 365 (793 municipalities). The 534 unclassified municipalities (5 %) are mostly behind gate-

Table 4: Country-level email security overview ($n = 15{,}306$ municipalities).

Country	n	SPF	gSPF[1]	DMARC	gDMARC[2]	DANE
Germany	11,105	87.5%	35.9%	50.7%	16.9%	1.6%
Austria	2,092	97.8%	62.2%	37.4%	3.3%	0.0%
Switzerland	2,109	99.2%	79.9%	55.5%	13.4%	7.3%
Total	15,306	**90.6%**	**45.6%**	**49.6%**	**14.5%**	**2.2%**

[1] Well-configured SPF (no overly permissive mechanisms).
[2] Well-configured DMARC (enforcement policy).

ways (Sophos, SecureMailGate, NoSpamProxy, Hornetsecurity). Bavaria is the clear outlier at 18.7 % US-cloud, followed by Hesse at 12.3 %. The city-states Hamburg, Bremen, and Berlin show 0 % US-cloud. Northern states with strong communal IT providers Schleswig-Holstein (2.4 %), Nordrhein-Westfalen (0.3 %) and Rheinland-Pfalz (2.9 %) have the lowest US-cloud shares.

Austria Austria shows the highest US-cloud dependency of the three countries: Microsoft 365 serves 67 % of 2,092 municipalities, with domestic providers covering only 29 %. For 3 % (51), the provider remains unclassified, predominantly due to gateways. The state-level variation is stark. Upper Austria 89 % and Tyrol 87 % are heavily Microsoft-dependent. At the opposite extreme, Burgenland and Carinthia route 95 %, resp. 97 % through a shared state IT provider.

Switzerland Microsoft 365 dominates Swiss municipal email with 52 % of 2,110 municipalities, followed by domestic providers at 42 %. Together with AWS (22) and Google (4), US-based cloud providers serve 53 % of all municipalities. For 4.4 % (93 municipalities), the provider could not be determined—in 89 of these cases because a security gateway obscures the underlying infrastructure. Cantonal variation is substantial: seven cantons (AR, AI, BS, GL, NE, NW, ZG) are entirely served by domestic providers. Geneva stands out with 98 % domestic coverage through the shared infrastructure of ACG Genève, a municipal association. Overall, 10 of the 26 cantons have a US-cloud share exceeding 50 %.

5.2 Security Posture

Germany 88 % of German municipalities have an SPF record, while only 36 % enforce a strict *-all* policy. DMARC is present on 50 % of domains, yet only 17 % enforce a *reject* policy. DANE is supported by very few municipalities (with a range of 0-3 %)—the only outlier being the state of Hesse, with 28 %.

Austria Nearly all Austrian municipalities (98 %) have an SPF record—62 % showing a good configuration. Only 3 % have DMARC with a *reject* policy in place (37 % have DMARC in place in total). No municipality supports DANE.

Switzerland SPF records are nearly universal (99 %), with 80 % enforcing a strict *-all* policy—the highest rate among the three countries. DMARC is present on 56 % domains, yet only 13 % employ a *reject* policy; nine cantons have no

enforcement at all, while Zug reaches 55 %. CH is the only country where DANE is present beyond isolated cases (7 %), carried largely by domestic providers.

6 Discussion

Germany As we have seen in Sect. 5.1, there are great differences in terms of US provider dependency between the states. It is not surprising to us that Bavaria (BY) has the highest dependency on US providers with 19 %—mostly on Microsoft. This is due to the fact that Microsoft's German headquarters (also the company's largest European foreign subsidiary) is based in Munich and the political will to introduce Microsoft in the public sector in Bavaria has been high for years. At the end of 2025, it became known that the Bavarian state government intended to conclude a contract for the use of the cloud-based office suite Microsoft 365 for the Bavarian public administration. According to a presentation by the Bavarian Ministry of Finance, obtained by Heise[3], the goal was to finalize a "new consolidated Enterprise Agreement (EA) for public authorities". Through the so-called "Bavaria contract", ministries and state authorities shall initially be enabled to use these services. On this basis, a subsequent "municipal contract" is planned for cities and municipalities. The presentation specifically identifies the M365 E5 package, including Teams, as the product in question, which represents Microsoft's most comprehensive and powerful licensing plan for large enterprises. Costs are estimated at around one billion Euros over the course of five years. In June 2026, Heise reported that the contract negotiations between Bavaria and Microsoft have been canceled.[4]

Hesse (HE) comes at the second place concerning US dependency in Germany. An explanation might be that Frankfurt, as an important international financial city with global institutions using more homogeneous infrastructure, has an impact on the state as a whole.

At the other end of the list, we have states in the northern part of Germany that have been following the path of digital sovereignty for years now. *Dataport* is a common IT service provider publicly run by several (northern) states. Especially the state of Schleswig-Holstein (SH), whose IT alliance for municipalities is also part of Dataport (additionally to the state level, which has been pushing consistently for an open-source strategy lately[5]), strikes out with its small US dependency of only 2.4 % (besides the two city states Hamburg (HH) and Bremen (HB), both being part of Dataport as well and both with zero US dependency).

Another interesting state is Rhineland-Palatinate (RP), which has also a very low US dependency of only 2.9 %. In this state, United Internet AG has its headquarters. IONOS, as one of the biggest European cloud and hosting

[3] https://www.heise.de/news/Vertrag-soll-bis-Jahresende-stehen-Bayern-will-in-die-Microsoft-Cloud-11066618.html

[4] https://www.heise.de/news/Bayern-Neuer-Microsoft-Deal-ist-vorerst-vom-Tisch-11316994.html

[5] https://www.heise.de/news/Schleswig-Holstein-Open-Source-ist-praxistauglich-trotz-Umstellungsproblemen-11131005.html

providers (especially targeting SMEs) is a direct subsidiary of United Internet AG. Furthermore, GMX and Web.de (two leading email providers in Austria, Germany, and Switzerland) are indirect subsidiaries of United Internet AG. It is no surprise that we have found numerous municipalities in RP that use one of the services provided by United Internet AG.

Furthermore, we have the states of Baden-Württemberg (BW), North Rhine-Westphalia (NW), and Sachsen (SN) that have strong communal IT providers and, thus, low US dependencies overall (3.5 % in BW, 3.6 % in SN, and 0.3 % in NW—where it is interesting to see that NW still shows the historic split of the state and we only find the high number of communal IT in the area of Westfalen).

Concerning the implemented security mechanisms, only few states (city states aside) have a good SPF policy in place above the level of 50 % of municipalities: BY, HE, NW. RP strikes out with the highest "good DMARC policy" of all states with 36 %. This result is due to the high number of customers of United Internet AG and especially GMX and Web.de pushing for the implementation of these mechanisms in practice. DANE implementation is still at a very low level, as expected—the only outlier is Hesse where 28 % of the municipalities are secured via DANE. This might be explicable because DENIC is based in Frankfurt and has actively promoted DNSSEC (the prerequisite protocol for DANE) since its introduction. Moreover, DE-CIX, one of the biggest Internet Exchange Points worldwide, is also based in Frankfurt and, thus, numerous network providers, DNS providers, and hosting providers are based in Frankfurt as well.

Austria Only two states in Austria have a centralized state email infrastructure: Burgenland and Carinthia. We could only determine that the municipalities in Burgenland are being hosted by a domestic provider with a confidence of 74 % (as performed according to the rule presented in Sect. 4.2), as we found that "messagelabs.com" (a Broadcom service) is allowed to send emails (according to the SPF entries). We received a confirmation by the responsible person from the *Gemeinde Servicezentrum* in Carinthia, which is responsible for hosting the email infrastructure for municipalities in Carinthia, that all services are provided in Austria by European service providers.

The differences between the states are substantial in terms of security measures in Austria. For example, the capital city Vienna does neither have a good SPF, nor a good DMARC policy in place—leaving its inhabitants (roughly 2 million) prone to spoofing attacks impersonating the city. On the other hand, Burgenland (the state with the lowest population, roughly 300,000 inhabitants) has the highest rate of "good SPF" cases with 95 % and 0 % "good DMARC" cases. As there are no clear instructions due to the missing DMARC entries, the decision how to deal with spoofed emails is left to the receiving email servers. In most cases, such emails will probably land in the spam folders, as this is the configuration typically found in practice. Styria (1.2 million inhabitants) shows the best results of all states with 87 % good SPF and 10 % good DMARC.

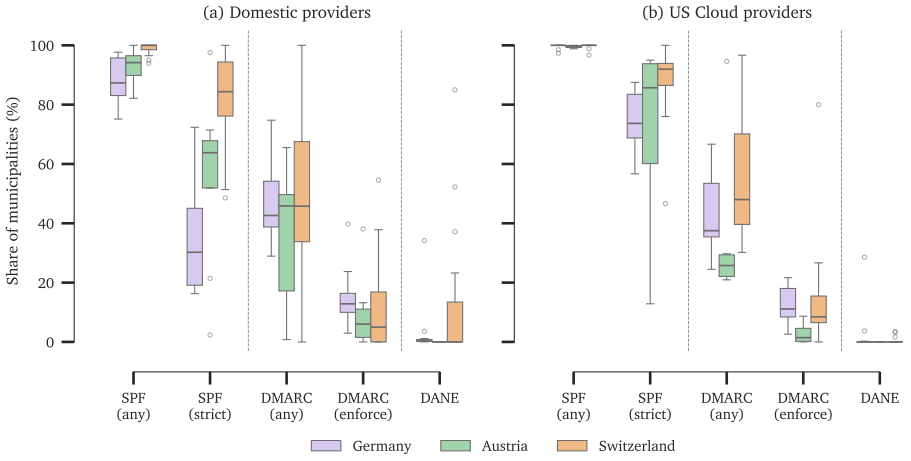

Fig. 2: Email security adoption by provider category.

Switzerland As Section 5.1 shows, US-cloud providers—predominantly Microsoft 365—serve 53 % of Swiss municipalities, while 42 % rely on domestic providers, with strong cantonal variation in both dimensions.

In the canton of Geneva, 44 of 45 municipalities share the ACG Genève infrastructure, with only the city of Geneva on Microsoft 365. Despite this near-complete domestic consolidation, the ACG platform has not deployed good DMARC for any of its member municipalities. Notably, in 2022 the canton's popular vote uniformly accepted with 94 % the right to digital integrity as a constitutional amendment (Art. 21A of the cantonal constitution), and other cantons have filed motions to various degrees as well. Geneva thus demonstrates that political commitment to digital sovereignty can coexist with gaps in the technical security of the very infrastructure that sovereignty seeks to protect.

Even in cantons with the highest Microsoft penetration—St. Gallen (80 %) and Aargau (75 %)—good DMARC remains low (21 % and 13 % respectively). Nationally, 87 % of Microsoft-using municipalities have not enabled a strict DMARC *reject* policy. Appenzell Ausserrhoden's single domestic provider achieves 95 % good SPF and 85 % DANE support, while Jura stands out with 39 % good DMARC despite a less concentrated provider mix.

Swiss `.ch` domains had historically a low DNSSEC adoption despite SWITCH (`.ch` registry operator) supporting it since 2010. A recent surge in 2021/2022 led to 51 % as of April 2026 [27]. Only 7 % of municipalities support DANE.

6.1 Defaults vs. Enforcement: Provider Effects on Security

The choice of providers shapes the security posture along two opposing axes: US Cloud platforms have secure defaults that are set when tenants are onboarded (SPF), while domestic providers lead in areas that require active configuration. Figure 2 aggregates municipalities to the state or canton level; chi-square tests of independence (n=14,456) confirm all five metrics are significantly associated with provider category ($p < 0.001$ in each case). First, US Cloud providers deliver

markedly higher well-configured SPF ($\chi^2(1) = 1456.4$): Microsoft 365 reaches 66–89 % across the three countries, whereas domestic providers reach only 33 % in Germany and 74 % in Switzerland—74 % of MS 365 municipalities publish an SPF record that authorizes Microsoft (`include:spf.protection.outlook.com`) with a strict `-all` qualifier.

Second, the opposite holds for DMARC enforcement: well-configured DMARC stays at or below 18 % everywhere, yet Domestic outperforms US Cloud in every country stratum (17.1 % vs 7.9 % pooled; MS/Domestic odds ratio 0.47–0.93), and only 17 % of MS 365 municipalities publishing DMARC reach a strict *reject* policy. Third, DANE is almost exclusively a domestic phenomenon and is highly concentrated: most regions show zero adoption, while a handful of Swiss cantons reach 20–85 %.

Security gateways add a further layer: routing through one raises DMARC presence by ∼10 % but lowers good SPF by ∼11 % ($p < 0.001$), with Austria leading at 37 % gateway adoption (predominantly SEPPmail).

7 Conclusion and Outlook

We have presented the first large-scale, cross-country measurement of email security and provider dependencies in municipal administrations, covering more than 15,000 domains across Germany, Austria, and Switzerland. Our open-source, country-agnostic three-stage pipeline—domain resolution, DNS-based provider fingerprinting, and active security scanning—reaches 97.2 % agreement with bounce-probe ground truth on a stratified sample of 398 municipalities, and is released with two interactive maps, one for provider attribution and one for security posture. We revealed national variations: Germany is predominantly domestic (87 %), while Austria and Switzerland have converged on US-based cloud platforms (67 % and 53 %, respectively). In all countries, SPF is used in 91 % of municipalities, yet only 46 % enforce a strict policy, DMARC *reject* is implemented only by 15 %, and adoption of DANE remains negligible at 2 %.

The gap is most prominent on hyperscaler platforms: of the 3,293 municipalities hosted on Exchange Online, only 17 (0.5 %) utilize DANE—and the provider effect is asymmetric, with US Cloud achieving high rates only on strict SPF, while domestic providers lead on the enforcement-requiring layers (roughly 2× the strict-DMARC rate of US Cloud in every country; 91 % of DANE support).

From a regulatory perspective, our results point to a gap between existing recommendations and their enforcement. The authority for entities such as BSI to actively enforce compliance is largely limited to critical infrastructure operators, whereas municipalities typically fall outside this scope. As a result, the adoption of recommended security measures in the municipal sector remains uneven. At the same time, recent developments indicate increasing efforts by public authorities to promote stronger adoption of email security mechanisms.

Our study is a point-in-time snapshot and cannot capture ongoing migrations. DKIM is excluded because its selectors are not globally enumerable, and on-premises gateways obscure a subset of backends. While we consider the non-

intrusiveness of collection methods to be a particular strength, digital sovereignty apparently extends beyond the public network signals we observe.

Continuous, data-driven evaluation is needed to assess whether national initiatives, such as the BSI's 2026 DNSSEC push, cantonal mandates, or Bavaria's municipal Microsoft contracts, translate into measurable improvements over time. We therefore plan longitudinal re-measurement and extension to further countries, and view our open-source pipeline and maps as an instrument the community can build on.

References

1. Blechschmidt, B., Stock, B.: Extended hell(o): A comprehensive Large-Scale study on email confidentiality and integrity mechanisms in the wild. In: 32nd USENIX Security Symposium (USENIX Security 23). pp. 4895–4912. USENIX Association, Anaheim, CA (Aug 2023), https://www.usenix.org/conference/usenixsecurity23/presentation/blechschmidt
2. Bresu: Liste österreichischer gemeinden inkl. e-mail & website (2022), https://github.com/bresu/oe_gemeinden, commit: eeaa42c
3. Christian Berendt: Email providers of german municipalities displayed on a map (2026), https://github.com/B42Labs/mxmap, commit: 7b0470c
4. Czybik, S., Horlboge, M., Rieck, K.: Lazy gatekeepers: a large-scale study on spf configuration in the wild. In: Proceedings of the 2023 ACM on Internet Measurement Conference. pp. 344–355 (2023). https://doi.org/10.1145/3618257.3624827
5. Falkner, G., Heidebrecht, S., Obendiek, A., Seidl, T.: Digital sovereignty-rhetoric and reality. Journal of European Public Policy **31**(8), 2099–2120 (2024). https://doi.org/10.1080/13501763.2024.2358984
6. Floridi, L.: The fight for digital sovereignty: What it is, and why it matters, especially for the EU. Philosophy & technology **33**(3), 369 (2020). https://doi.org/10.1007/s13347-020-00423-6
7. Fratini, S., Hine, E., Novelli, C., Roberts, H., Floridi, L.: Digital sovereignty: A descriptive analysis and a critical evaluation of existing models. Digital Society **3**(3), 59 (2024). https://doi.org/10.1007/s44206-024-00146-7
8. Hager, T., Petrlic, R.: The Fragility of DNS-Based Security Under Imperfect DNS Operation. In: Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb). Internet Society (2026). https://doi.org/10.14722/madweb.2026.23041
9. Hu, H., Wang, G.: End-to-End measurements of email spoofing attacks. In: 27th USENIX Security Symposium (USENIX Security 18). pp. 1095–1112. USENIX Association, Baltimore, MD (Aug 2018), https://www.usenix.org/conference/usenixsecurity18/presentation/hu
10. Hureau, O., Bayer, J., Duda, A., Korczyński, M.: Spoofed emails: An analysis of the issues hindering a larger deployment of dmarc. In: International Conference on Passive and Active Network Measurement. pp. 232–261. Springer (2024). https://doi.org/10.1007/978-3-031-56249-5_10
11. Ilja Livenson: Mx map — email providers of municipalities worldwide (2026), https://github.com/livenson/mxmap, commit: 9663a4a
12. Lange, C., Chang, T., Fiedler, M., Petrlic, R.: An email a day could give your health data away. In: Garcia-Alfaro, J., Navarro-Arribas, G., Dragoni, N. (eds.) Data

Privacy Mgmt, Cryptoc. and Blockchain Techn. pp. 53–68. Springer International Publishing, Cham (2023). https://doi.org/10.1007/978-3-031-25734-6_4
13. Lee, H., Girish, A., Van Rijswijk-Deij, R., Kwon, T., Chung, T.: A longitudinal and compr. study of the dane ecosystem in email. In: Proceedings of the 29th USENIX Conference on Security Symposium. SEC'20, USENIX Association, USA (2020)
14. Liu, E., Akiwate, G., Jonker, M., Mirian, A., Ho, G., Voelker, G.M., Savage, S.: Forward pass: On the security implications of email forwarding mechanism and policy. In: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P). pp. 373–391. IEEE, Delft, Netherlands (2023). https://doi.org/10.1109/EuroSP57164.2023.00030
15. Liu, E., Akiwate, G., Jonker, M., Mirian, A., Savage, S., Voelker, G.M.: Who's got your mail?: characterizing mail service provider usage. In: Proceedings of the 21st ACM Internet Measurement Conference. pp. 122–136. ACM, Virtual Event (Nov 2021). https://doi.org/10.1145/3487552.3487820
16. Mahendru, S., Pandit, T.: Securenet: A comparative study of deberta and large language models for phishing detection. In: 2024 IEEE 7th International Conference on Big Data and Artificial Intelligence (BDAI). pp. 160–169. IEEE (2024). https://doi.org/10.1109/BDAI62182.2024.10692765
17. Martínez-Ramil, P., Bolaños-Frasquet, H., Hamuľák, O., Kerikmäe, T.: A multidimensional understanding of EU's digital sovereignty. In: Ramiro Troitiño, D., Kerikmäe, T., Hamuľák, O. (eds.) Digital Development of the European Union: An Interdisciplinary Perspective, pp. 235–247. Springer (2023). https://doi.org/10.1007/978-3-031-27312-4_15
18. National Cyber Security Centre (NCSC): Anti-phishing report 2024. Tech. rep., Swiss Confederation (2025), `https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/antiphishing2024.html`, acc.: 2026-04-14
19. National Cyber Security Centre (NCSC): Mandatory reporting for cyberattacks on crit. infrastr. (2025), `https://www.report.ncsc.admin.ch/en/`, acc.: 2026-04-14
20. National Cyber Security Centre (NCSC): Semi-annual report 2024/2. Tech. rep., Swiss Conf. (2025), `https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/berichte/lageberichte/halbjahresbericht-2024-2.html`, acc.: 2026-04-14
21. OpenPLZ: API (2026), `https://www.openplzapi.org/en/`, accessed: 2026-04-04
22. privatim: Resolution zur auslagerung von datenbearbeitungen in die cloud (2025), `https://www.privatim.ch/wp-content/uploads/2025/11/20251124_privatim_Resolution-Hyperscaler_DE.pdf`, november 24, 2025. Acc.: 2026-04-16
23. Qi, Q., Luo, Y., Xu, Y., Guo, W., Fang, Y.: Spearbot: Leveraging large language models in a generative-critique framework for spear-phishing email generation. Information Fusion **122**, 103176 (2025). https://doi.org/10.1016/j.inffus.2025.103176
24. Ribeiro, D., Fonte, V., Ramos, L.F., Silva, J.M.: Assessing the information security posture of online public services worldwide: Technical insights, trends, and policy implications. Government Information Quarterly **42**(2) (2025). https://doi.org/10.1016/j.giq.2025.102031
25. Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., Floridi, L.: Safeguarding european values with digital sovereignty: An analysis of statements and policies. Internet Policy Review (2021). https://doi.org/10.2139/ssrn.3937345
26. Swiss Federal Government: Applikation der schweizer gemeinden (2026), `https://www.agvchapp.bfs.admin.ch/de`, accessed: 2026-04-04
27. SWITCH: .ch domain names with dnssec (2026), `https://www.nic.ch/statistics/dnssec/`, accessed: 2026-04-08
28. SWITCH: DNS resil. prog. (2026), `https://www.nic.ch/security/resilience/`, measurem. at `https://dns-resilience.openintel.nl/`. Acc.: 2026-04-14

29. T. Cymru: IP to ASN lookup (2024), https://asn.cymru.com/, acc.: 2026-04-08
30. Tan, K.L., Chi, C.H., Lam, K.Y.: Survey on digital sovereignty and identity: From digitization to digitalization. ACM Comput. Surv. **56**(3) (Oct 2023). https://doi.org/10.1145/3616400
31. Tatang, D., Zettl, F., Holz, T.: The evolution of dns-based email authentication: Measuring adoption and finding flaws. In: Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses. pp. 354–369. RAID '21, Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3471621.3471842
32. The Federal Assembly of the Swiss Confederation: Federal act on data protection (FADP), https://www.fedlex.admin.ch/eli/cc/2022/491/en, sR 235.1. Acc.: 2026-04-14

A Maps for Provider and Security by Municipality

The interactive can be found at `https://secassure2026.mxmap-project.org/`.

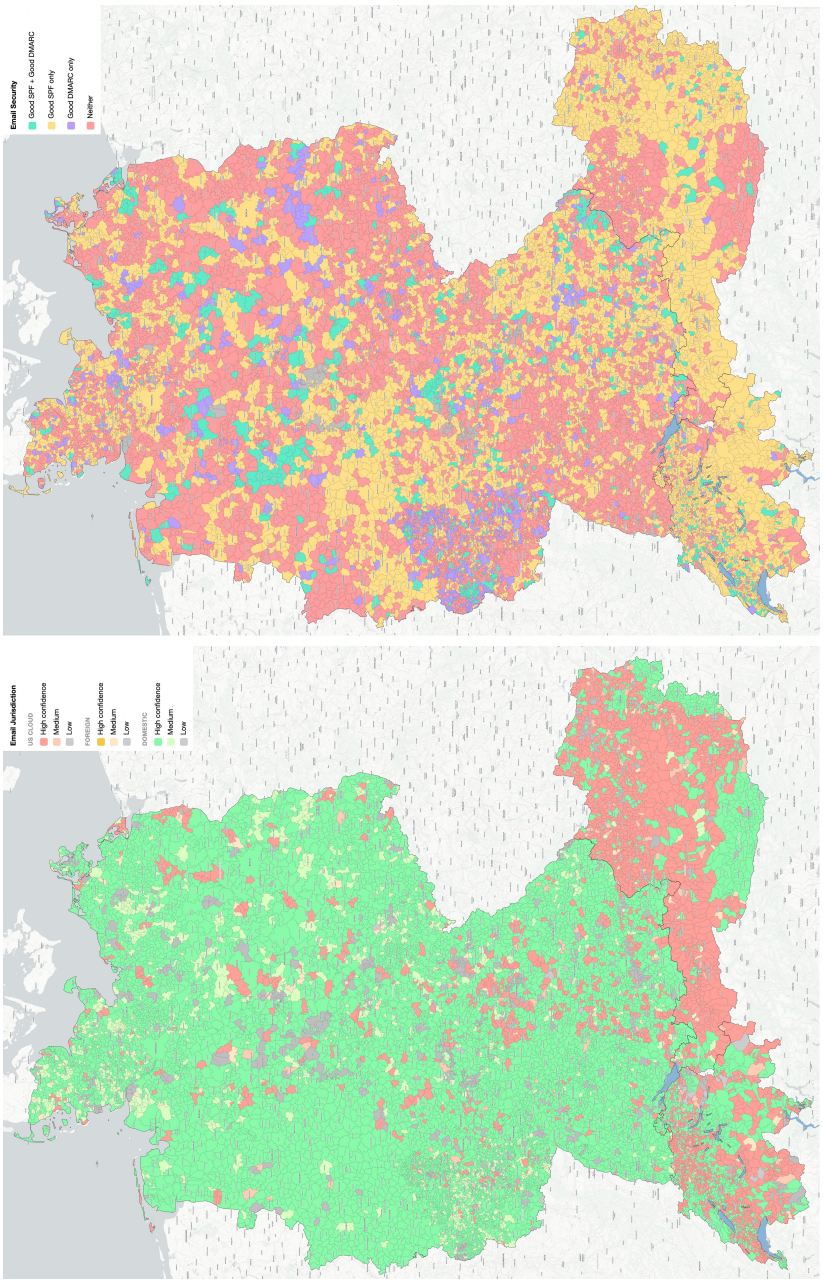

Fig. 3: Email providers and email security for Germany, Austria and Switzerland

B Provider and Security Results by Region

Code and dataset can be accessed at `https://github.com/mxmap/secassure2026`.

Table 5: Provider Distribution and Email Security Adoption by Region

	Provider (Absolute & %)									Security (Adoption %)				
Region	$\sum$	**MS**	**GO**	**AZ**	**Dom**	**Frg**	**Unk**	**Dom**	**US**	**S**	**gS**	**DM**	**gDM**	**DN**
Bad.-Württ.	1098	38	0	0	1014	0	46	92.3	3.5	97.4	18.9	74.5	3.2	0.1
Bayern	2055	384	1	0	1563	12	95	76.1	18.7	93.7	56.3	43.1	14.1	0.5
Berlin	1	0	0	0	1	0	0	100.0	0.0	100.0	100.0	100.0	0.0	0.0
Brandenburg	417	32	0	0	366	5	14	87.8	7.7	84.8	26.0	50.4	16.9	3.1
Bremen	2	0	0	0	2	0	0	100.0	0.0	100.0	0.0	100.0	0.0	0.0
Hamburg	1	0	0	0	1	0	0	100.0	0.0	100.0	100.0	100.0	0.0	0.0
Hessen	423	52	0	0	351	0	20	83.0	12.3	97.2	72.3	41.4	11.3	28.4
Meckl.-Vorp.	767	60	0	0	652	7	48	85.0	7.8	87.3	39.9	39.7	12.5	0.3
NRW	396	1	0	0	389	0	6	98.2	0.3	97.7	52.8	70.2	13.4	0.5
Niedersachs.	975	50	1	0	860	15	49	88.2	5.2	88.2	32.0	53.1	12.3	0.3
Rheinl.-Pf.	2302	63	4	0	2053	58	124	89.2	2.9	80.4	21.6	63.6	36.3	0.2
Saarland	52	2	0	0	47	0	3	90.4	3.8	96.2	30.8	36.5	7.7	0.0
Sachs.-Anh.	221	21	0	0	177	5	18	80.1	9.5	79.1	38.6	42.3	23.2	3.6
Sachsen	439	16	0	0	408	5	10	92.9	3.6	87.7	19.2	29.2	7.1	0.2
Schles.-Hol.	1110	26	1	0	1001	30	52	90.2	2.4	78.2	44.8	36.0	12.1	0.6
Thüringen	870	48	1	0	762	10	49	87.6	5.6	84.0	24.0	40.1	13.1	0.8
DE	**11129**	**793**	**8**	**0**	**9647**	**147**	**534**	**86.7**	**7.2**	**87.5**	**35.9**	**50.7**	**16.9**	**1.6**
Burgenland	171	3	0	0	163	4	1	95.3	1.8	99.4	95.3	3.5	0.0	0.0
Kärnten	132	2	0	0	128	0	2	97.0	1.5	100.0	3.8	2.3	0.8	0.0
Niederöst.	573	425	0	0	112	9	27	19.5	74.2	97.7	74.2	26.9	3.1	0.0
Oberösterr.	438	389	0	0	41	4	4	9.4	88.8	99.1	17.8	90.2	1.1	0.0
Salzburg	119	86	0	0	29	1	3	24.4	72.3	97.5	84.0	31.9	2.5	0.0
Steiermark	285	219	0	0	53	6	7	18.6	76.8	97.2	87.7	28.1	10.2	0.0
Tirol	277	240	0	0	21	10	6	7.6	86.6	97.8	89.2	24.5	3.2	0.0
Vorarlberg	96	37	0	0	56	2	1	58.3	38.5	89.6	35.4	40.6	3.1	0.0
Wien	1	0	0	0	1	0	0	100.0	0.0	100.0	0.0	0.0	0.0	0.0
AT	**2092**	**1401**	**0**	**0**	**604**	**36**	**51**	**28.9**	**67.0**	**97.8**	**62.2**	**37.4**	**3.3**	**0.0**
Aargau	231	162	0	12	52	0	5	22.5	75.3	99.1	87.4	60.2	12.6	3.5
Appenzell A.	20	0	0	0	20	0	0	100.0	0.0	95.0	95.0	95.0	5.0	85.0
Appenzell I.	5	0	0	0	5	0	0	100.0	0.0	100.0	100.0	0.0	0.0	0.0
Basel-Land	86	58	0	3	23	0	2	26.7	70.9	97.7	81.4	68.6	10.5	3.5
Basel-Stadt	3	0	0	0	3	0	0	100.0	0.0	100.0	33.3	100.0	0.0	0.0
Bern	334	161	0	6	147	5	15	44.0	50.0	98.8	77.2	59.0	14.1	9.6
Freiburg	119	83	0	0	33	0	3	27.7	69.7	98.3	89.1	36.1	14.3	5.0
Genf	45	1	0	0	44	0	0	97.8	2.2	100.0	95.6	24.4	0.0	0.0
Glarus	3	0	0	0	3	0	0	100.0	0.0	100.0	100.0	0.0	0.0	0.0
Graubünden	82	50	0	0	32	0	0	39.0	61.0	100.0	92.7	45.1	6.1	1.2
Jura	51	15	0	0	35	0	1	68.6	29.4	100.0	64.7	76.5	39.2	25.5
Luzern	51	24	1	0	26	0	0	51.0	49.0	100.0	76.5	68.6	11.8	0.0
Neuenburg	24	0	0	0	24	0	0	100.0	0.0	100.0	100.0	100.0	0.0	0.0
Nidwalden	11	0	0	0	11	0	0	100.0	0.0	100.0	90.9	18.2	0.0	0.0
Obwalden	7	1	0	0	6	0	0	85.7	14.3	100.0	100.0	14.3	0.0	0.0
Schaffhausen	26	6	0	0	20	0	0	76.9	23.1	100.0	92.3	30.8	0.0	0.0
Schwyz	30	3	0	0	22	0	5	73.3	10.0	100.0	90.0	80.0	0.0	0.0
Solothurn	104	70	0	1	29	4	0	27.9	68.3	99.0	79.8	49.0	9.6	1.0
St. Gallen	75	60	0	0	1	0	14	1.3	80.0	100.0	40.0	94.7	21.3	2.7
Tessin	100	53	0	0	45	1	1	45.0	53.0	99.0	84.0	36.0	4.0	2.0
Thurgau	80	20	0	0	57	0	3	71.2	25.0	97.5	82.5	60.0	10.0	0.0
Uri	19	3	0	0	16	0	0	84.2	15.8	100.0	94.7	26.3	5.3	0.0
Waadt	300	177	2	0	111	3	7	37.0	59.7	99.7	74.9	52.8	27.8	19.4
Wallis	142	84	0	0	43	1	14	30.3	59.2	99.3	78.2	43.7	10.6	7.0
Zug	11	0	0	0	11	0	0	100.0	0.0	100.0	90.9	63.6	54.5	0.0
Zürich	151	68	1	0	59	0	23	39.1	45.7	100.0	74.2	60.3	3.3	0.0
CH	**2110**	**1099**	**4**	**22**	**878**	**14**	**93**	**41.6**	**53.3**	**99.2**	**79.9**	**55.5**	**13.4**	**7.3**
Grand Tot.	**15331**	**3293**	**12**	**22**	**11129**	**197**	**678**	**72.6**	**21.7**	**90.6**	**45.6**	**49.6**	**14.5**	**2.2**

MS Microsoft, **GO** Google, **AZ** Amazon, **Dom** Domestic, **Frg** Foreign, **Unk** Unknown;
S SPF, **gS** good SPF, **DM** DMARC, **gDM** good DMARC, **DN** DANE.

≥80% 50–79% <50% — domestic share (provider) resp. adoption (security).