

Insight

Dawn raids: preparing for the knock on the door

Dawn raids have become a standard enforcement tool in Switzerland, affecting both suspects and third parties. In this age of big data, proper preparation is vital in preventing procedural missteps, uncontrolled data disclosure and irreversible exposure.

Dawn raids: The “new normal”

Dawn raids are on the rise. What was once conceptualised as an *ultima ratio* coercive measure for obtaining evidence is becoming a standard entry point into complex criminal investigations – in other words, a standard Swiss enforcement practice.

In transnational cases, evidence is often fragmented across jurisdictions, cloud infrastructures and digital platforms. Evidence gathering can be a lengthy process, with dawn raids offering authorities a swift and effective means of securing large volumes of data at an early state of the investigation.

This development is reinforced by a judicial trend in the Swiss courts. Since the courts generally side with the authorities when assessing the legality of such measures, challenging dawn raids has become progressively more difficult.

Now more than ever, preparation and strategic readiness are essential, should the authorities come knocking.

Becoming an inadvertent target

One common misconception is that only suspects can be targeted by dawn raids.

Under Swiss law, a dawn raid may also be directed against third parties where relevant evidence is expected to be found. In practice, this expands the perimeter significantly. Service providers, group entities, fiduciaries, IT hosts, compliance consultants – and even business partners – may find their premises being searched, despite not being accused of any wrongdoing.

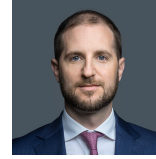
The implications of this are twofold. Third parties bear a substantial financial and procedural burden, since protecting privileged and confidential information under acute time pressure is procedurally complex and costly. They also face unwarranted exposure by being drawn into criminal proceedings without being accused of wrongdoing at the outset. Incidental findings may subsequently shift their position within the investigation, transforming them from mere data holders into potential suspects.

Data as the battlefield

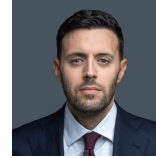
Today, dawn raids go beyond paper files and physical archives. They are centred on forensic data extraction at scale.

Authorities will secure entire devices or servers and vast volumes of digital data first – and discuss scope and relevance later. This approach shifts the

Authors



Benoît A Mauron
Partner
Geneva



Adam El-Hakim
Partner
Zurich



Nikita Ognitvsev
Counsel
Geneva



Vivien Altwegg
Associate
Zurich

“Proper preparation demands more than having a well-written policy theoretically available to employees. It is about technical, organisational and strategic readiness”

burden of proof to the data holder and often triggers protracted and technically demanding disputes over the disclosure and scope of the secured data.

Walking the tightrope between confrontation and co-operation

In this context, the right of the data holder to request the sealing of secured data, subject to substantiation and confined by judicial practice, is an important procedural instrument to preserve privilege and contain scope.

At the same time, unsealing proceedings have grown increasingly complex. Swiss courts demand granular justification of sealing grounds and expect precise identification of protected data. In practice, this resembles standalone litigation, demanding both technical command of the data and a firm understanding of the evolving Swiss procedural and jurisdictional landscape. Any missteps at this stage can irreversibly shape the evidentiary landscape of the investigation.

Swiss practice leaves room for extra-judicial agreements, and negotiated solutions (covering data scoping, filtering, review, and cross-border co-ordination) can offer a pragmatic alternative to lengthy court proceedings. The voluntary disclosure of passcodes often works as a bargaining chip in this respect. The growing relevance of such negotiated outcomes reflects a broader reality: measured co-operation, when strategically managed, can reduce friction and limit exposure for all parties involved.

Preparation is more than a policy paper

Proper preparation demands more than having a well-written policy theoretically available to employees. It is about technical, organisational and strategic readiness:

1. *Data organisation*: it is essential to have a clear and well-mapped overview of the data and where it is stored. A structured file management system and centralised file inventories will contribute to a smooth and regulated search by the authorities. This helps contain scope and may prevent unrelated incidental findings. Any privileged material should likewise be clearly identified in the file management system.
2. *Data control*: unrestricted access to data (e.g. cloud environments and messaging platforms) can irreversibly expand the scope of an investigation. Uncoordinated internal actions or ill-considered “clean-up” attempts may create additional exposure. Clear rules governing who has access to which systems and devices, coupled with accessibility restrictions and password protection, are essential to maintain data control and restrict scope. The disclosure of passwords and credentials may also be used as a strategic bargaining chip.
3. *Response team and trainings*: dawn raids are disruptive by nature. Response team roles and responsibilities must be defined in advance, ranging from the on-site engagement with the authorities to external and internal communication. Effective response depends on a predefined crisis governance structure that enables swift, co-ordinated decision-making under pressure. Targeted training ensures that employees understand the applicable protocols and can implement them under pressure.
4. *Operational resilience*: having operational measures in place to ensure immediate business continuity is key. Operational resilience relies on clear internal communication protocols, uninterrupted access to critical IT systems and the ability to continue managing the payroll; making payments to suppliers, and carrying on core operations even if data is partially seized. Companies should also manage customer and supplier communications in a

timely manner to avoid contractual breaches and reputational damage.

5. *External assistance*: The trajectory of the investigation will be shaped by the initial response. Timely and experienced legal guidance is critical in controlling data disclosure, protecting privilege and preventing complexity from turning into irreversible exposure. Proper media response assistance will also help mitigate reputational risks.

In a fast-evolving enforcement environment characterised by coercive, data-driven evidence gathering and heightened procedural pressure, dawn raid readiness can no longer be regarded a tick-box compliance exercise: it should be treated as a central element of legal risk management.