DISCRETION BY DESIGN · CONFIDENTIAL CLIENT DELIVERABLE

The Mirror

Digital exposure audit

SAMPLE · REDACTED

Engagement ID	PI-M-2026-0387
Subject reference	M.V. (full name redacted on this sample)
Engagement type	The Mirror · €595 fixed
Delivery date	12 May 2026
Report length	25 pages including appendix
Classification	Client eyes only · see §A.3 handling
Analyst	PI Solutions analyst team (anonymous-analyst posture)
Data purge	All raw data purged 48h after delivery · see /data-purge-policy

PI. SOLUTIONS
privacyinsightsolutions.com · enquiries@privacyinsightsolutions.com

About this sample

What you are reading and why every finding is partially redacted.

The format is real. The subject is not.

This is a fully structured Mirror report in the exact format a real client receives. It is not a stripped-down marketing version. The methodology section, the per-category findings, the risk synthesis, the prioritised action plan, and the appendix all match what is delivered under engagement.

The subject — a senior management consultant based in Frankfurt — is fictional. The findings are constructed to reflect a realistic moderate-exposure profile for a professional at this seniority in the German market in 2026, drawing on the patterns we see in our work. No real person's data appears anywhere in this document.

Why the redactions remain

Even with a fictional subject, we apply our standard sanitisation: every email address, username, URL, street-level address, and credential fragment is partially blacked out. Three reasons. First, it shows you how a real deliverable looks if a third party ever sees it — a partner, a counsel, an auditor. Second, fictional identifiers can accidentally collide with real ones; redaction removes that risk. Third, the discipline is the brand: a privacy firm that ships unredacted sample reports has misunderstood its own positioning.

What you can still see

The **analytical content** — the broker names, the breach names, the dates, the severity scoring, the analyst reasoning, the recommended action — is visible in full. Those are the parts that demonstrate the work. The **subject-identifying fragments** — the email local-parts, the addresses, the cracked password strings, the platform handles — are the parts a real client would expect redacted before any third-party reading.

WHAT THE MIRROR DELIVERS

Engagement type	The Mirror — foundational digital exposure audit
Price	€595 fixed
Delivery	48 hours from intake confirmation
Format	Structured PDF report, per-category risk scoring, prioritised actions
Inputs needed	Name, one or more email addresses, one or more usernames (aliases accepted)
Hand-off	Findings carry forward to The Lockdown, The Shield, or The Eraser at no rework cost

Executive summary

Investigation of subject M.V., conducted 12 May 2026.

OVERALL EXPOSURE — HIGH

Across seven investigation categories, M.V.'s footprint sits in the **moderate-to-high** band for a German professional at partner level. The public-facing surface — LinkedIn, the firm directory — is well-managed. The exposure concentrates in three places the subject is unlikely to have looked at recently:

01 Forgotten accounts on platforms the subject no longer uses, still publicly indexed. — MEDIUM

02 Old email addresses appearing in **four** documented public breaches between 2012 and 2019, with at least one credential pair still circulating. — HIGH

03 Two German people-search platforms surface the subject's name with city, age band, and associated relatives — assembled from public records without consent. — HIGH

What this means in practice

A motivated researcher — a journalist, a competitor's due-diligence team, a social engineer building a spear-phishing pretext — could in under two hours assemble: the subject's current employer and seniority; one current home city; an age band; the names of at least two family members; a personal email address; and a credential pair that has appeared in at least one large credential-stuffing list. None of this required dark web access. All of it was reachable from public sources.

Categories examined	7
Distinct findings recorded	23
High-severity findings	6
Confirmed breaches with credential exposure	4
People-search platforms surfacing the subject	5
Recommended immediate actions (within 7 days)	4

Methodology & scope

What we did, what we did not, and why each line is drawn where it is.

The four-stage gated process

Every Mirror engagement runs through the same four stages. No stage proceeds until the previous stage has cleared analyst review.

01	**Discovery**	Brokers · breaches · social platforms · forums · search engines
02	**Cross-reference**	Identifier triangulation: usernames, emails, photos, biographical anchors
03	**Verification**	Every claimed finding re-confirmed by a second analyst before inclusion
04	**Report**	Structured PDF · per-category risk scoring · prioritised action plan

Inputs received from the subject

At intake on 12 May 2026 (minus 48 hours), M.V. provided: one current professional email, one historic personal email, two usernames the subject recalled using between 2002 and 2014, and the subject's full name and approximate year of birth.

No passwords, identity documents, or financial information were requested or accepted. Mirror engagements operate on a first-party consent model: the subject authorises investigation of their own footprint using lawful OSINT methods.

Categories investigated

01	Username & account discovery	Yes — full scope
02	Google trace & account mapping	Yes — pages 1–5 of name and variant searches
03	Social media profile assessment	Yes — public surface only, no platform-internal access
04	Profile photo reverse image search	Yes — three reference images cross-checked
05	Dark web & breach database exposure	Yes — five commercial breach indices + HIBP
06	Data broker & people-search assessment	Yes — German + cross-border platforms
07	Public records	Limited — see §A.2 (DE registry access closed)

Out of scope

Active dark web infiltration. The Mirror queries breach indices that aggregate leaked credentials; it does not run infiltration of forum markets or vendor channels. That work falls under The Lockdown.

Active data broker removal. The Mirror identifies broker exposure and provides opt-out guidance. Manual removal across 150+ brokers and people-search platforms is the scope of The Eraser.

Threat actor profiling. Where this report flags an adversary pattern, scope is limited to noting the pattern. Structured threat investigation is the scope of The Shield.

Findings overview

All 23 findings, grouped by investigation category, ranked by severity.

At-a-glance heatmap

Each column counts findings of that severity within the category. Hover columns are read left-to-right: **critical** first, then high, medium, low. Cells in mono numerals are exact counts.

Category	Crit	High	Med	Low	Headline
01 · Username & account discovery	0	1	3	1	Forgotten accounts on three legacy platforms remain publicly findable.
02 · Google trace & account mapping	0	0	2	2	Page 1 results well-managed; page 2–3 surface older affiliations.
03 · Social media profile assessment	0	1	2	1	LinkedIn well-curated; an old Twitter account remains discoverable.
04 · Profile photo reverse image search	0	0	1	1	Headshot has propagated to three secondary professional listings.
05 · Dark web & breach database exposure	0	3	1	0	Four documented public breaches contain the subject's historic addresses.
06 · Data broker & people-search	0	1	1	0	Two German people-search platforms surface assembled biographical data.
07 · Public records	0	0	0	1	Effectively closed under German law — see §07 for jurisdictional analysis.

How to read this report

Each of the seven categories that follows is a self-contained section. Findings within a section are numbered M-001 through M-023 and are listed in descending severity. Every finding carries a severity pill, a one-line title, a redacted evidence block, and an analyst note where the finding does not stand alone. Section 09 (Risk Synthesis) explains how the findings combine into a targeting profile. Section 10 is the prioritised action plan.

01 · Username & account discovery

Tracing reused usernames across platforms — the identifier most likely to bridge the subject's professional and personal footprints.

What we looked for

Two usernames were provided at intake: a short alphanumeric handle the subject recalled using on technical forums in the early 2000s, and a name-derived handle used across consumer platforms from approximately 2008 onward. Both were checked against a standard set of 312 platforms including social networks, forums, gaming platforms, code repositories, photo-sharing sites, and consumer marketplaces.

Why usernames matter. A username is the single most efficient identifier for an OSINT investigator because it tends to be reused. An adversary who learns one handle can, in most cases, find every account the subject created using it — without needing the subject's name, email address, or photograph.

Findings

M-001 HIGH **Legacy technical forum account bridges personal and professional identity**

Handle `mv[redacted]` was located on a German-language technical forum with a registration date in 2003. The associated profile lists a real-name field containing the subject's surname, links a personal email at `@[redacted]`, and shows 47 posts between 2003 and 2011. Two posts include geographic identifiers (a meet-up location and a referenced employer at the time) that match the subject's biography.

The same handle resolves on two further platforms: a gaming forum (last activity 2009) and an early blogging platform (dormant since 2007 but profile still indexed).

> **ANALYST NOTE** This is the single most consequential username finding. A user-search across three platforms starting from this handle alone returns: a real surname, two historic email addresses, an approximate age, and a former employer. Together these are enough to seed every subsequent investigation an adversary would run. Recommendation: account deletion or username change on all three platforms (see §10, action I-2).

M-002 MEDIUM **Dormant gaming-platform account remains publicly indexed**

Handle `mv[redacted]` resolves on a major gaming platform with a public profile page. The account shows no activity since 2014 but the profile remains discoverable via search, lists an avatar derived from the subject's LinkedIn headshot, and exposes a friends list of 23 accounts — three of which are tagged with first-name + last-initial labels that, via reverse-search, resolve to identifiable family members.

> **ANALYST NOTE** The exposure here is the friends list, not the account itself. The friends list provides three named relatives at one remove from the subject. See finding M-019 (people-search platforms) where two of these names re-appear in associated-persons records.

M-003 MEDIUM **Public code-repository profile exposes work email**

A public profile on a major code-hosting platform shows handle `v[redacted]` with no recent commits but with the subject's current professional email address `[redacted].com` set as the contact email on five public commits authored between 2017 and 2019. This is mineable by automated tools that scrape commit metadata.

> **ANALYST NOTE** Common pattern for consultants who maintained side projects during a junior role. Recommendation: change the commit email retroactively (the platform supports this) and set a no-reply email as default going forward.

M-004 MEDIUM **Reused username on consumer marketplace platforms**

Handle mv[redacted] resolves on two consumer marketplace platforms (one second-hand goods, one accommodation rental). Both profiles are dormant but show review histories that, in combination, indicate prior residence in a specific German postcode area and approximate dates of moves.

ANALYST NOTE Marketplace reviews are an underrated source of historic location data. They tend to be public, indexed by Google, and rarely deleted by users.

M-005 LOW **Photo-sharing platform account, locked but discoverable**

Handle m[redacted] exists on a major photo-sharing platform with a private (locked) account. The account is not viewable but is discoverable via name search and the profile photo is the same headshot used on LinkedIn — linking the locked private account to the public professional identity.

ANALYST NOTE The account itself leaks nothing. The link between professional identity and a private personal account leaks the existence of a private account, which can be a pretext anchor for social engineering.

02 · Google trace & account mapping

What surfaces when an investigator searches the subject's name, name variants, and known email addresses across major search engines.

Method

Searches conducted: full name; full name plus city; full name plus current employer (name only, never employer name in a way that would identify the firm publicly); surname plus first initial; both historic email addresses; both usernames. Results examined to depth of three result pages per query, plus image results, plus cached-page recovery via the Wayback Machine where original pages had been taken down.

Page 1 — well-managed

Page 1 results for the subject's full name return: the firm's consultant directory page, the subject's LinkedIn profile, two industry conference listings where the subject presented between 2021 and 2024, and one professional association membership page. All four first-page results are professional, accurate, and on-brand for a consultant at this level. **This is a positive finding**: page-1 results are what a typical due-diligence party will see, and they confirm the subject's seniority without leaking personal data.

Findings

M-006 MEDIUM **Wayback Machine retains content removed from the live web**

Three pages that have been taken down from the live web remain accessible via the Wayback Machine. Specifically: a 2009 university alumni page listing the subject with then-current contact details at [redacted].de; a 2013 industry-association directory page with a then-current employer (a different firm than the subject's current one); and a 2016 conference programme listing the subject's session topic and a personal mobile number (now disconnected, but still indexed).

ANALYST NOTE The Wayback Machine cannot be 'opted out of' in the same way live pages can. Pages can be requested for removal but the request is not always honoured, and even when honoured the page may remain cached in commercial archive services. Recommendation: identify which content is most consequential and pursue removal where possible, but treat archive presence as a permanent consideration rather than a fixable problem.

M-007 MEDIUM **Image search surfaces speaker portrait from third-party site**

Google Images returns the subject's LinkedIn headshot at high resolution as the second image result. The source is not LinkedIn itself but a 2022 industry-event website which republished the photo as part of a speaker biography. The third-party page also lists the subject's then-current professional email — a different address than the subject's current one, but indexed and reachable.

M-008 LOW **Pages 2–3 surface old affiliations but no exploitable data**

Pages 2 and 3 of the name-search return: a 2015 podcast appearance (academic content, not personal); a citation in an EU policy white paper (the subject is named as a contributor); an academic publication co-authorship (university research collaboration, biography content only); and a 2012 conference proceedings entry that includes the subject's university email at the time, long since deactivated.

ANALYST NOTE These results are not high-severity because the data is professional, dated, and contains no current contact information. They are noted because, in aggregate, they make the subject easy to verify as a real individual with a continuous professional history — useful to a social engineer building a credible pretext.

M-009 LOW **Email-search returns alumni directory caches**

Direct Google search for the subject's historic personal email m[redacted] returns three cached alumni directory pages. None expose the subject's current address or employer; all confirm year of university completion and the institution attended.

03 · Social media profile assessment

Public surface only: what an unauthenticated visitor can see, what is scrapeable, and what each platform exposes in aggregate.

Platforms reviewed

Platform	Status	Last activity	Finding reference
LinkedIn	Well-managed	Current	Detailed below — see M-010
Xing	Stale	Last 2019	Old job title and city, see M-011
X / Twitter	Discoverable	Last 2018	Discoverable via name + headshot, see M-012
Facebook	Locked	Active	Private — discoverable via name, see M-013
Instagram	Locked	Active	Private — see M-005 (cross-ref)
YouTube	None found	–	No account surfaced
Mastodon	None found	–	No account surfaced
TikTok	None found	–	No account surfaced

Findings

M-010 LOW **LinkedIn — well-curated, no exploitable detail**

Current LinkedIn profile lists the subject's current role, employer, and tenure. No personal mobile, personal email, family details, or home location. Connection count is in the typical range for the seniority. Recommendations under public posts are professional and recent.

This is a positive finding. The LinkedIn presence is consistent with the subject's public role and exposes nothing beyond it. Specifically, no contact details that would let an outsider reach the subject privately are visible.

M-011 MEDIUM **Xing profile retains stale role and city**

A Xing profile (the European equivalent professional network) was located and is publicly visible. Last updated 2019. Lists the subject's previous employer (different from the current one) and city of residence at the time. Photo is an older version of the subject's LinkedIn headshot.

ANALYST NOTE Stale professional profiles are an under-considered risk. A due-diligence party encountering both the current LinkedIn and the older Xing can reconstruct the subject's career timeline including job changes and their dates. Recommendation: either update or delete the Xing profile (action S-3 in §10).

M-012 HIGH **Old Twitter account remains discoverable, contains personal content**

Account @mv[redacted] exists on X / Twitter. Last tweet: November 2018. The account was used between 2010 and 2018 and contains approximately 2,300 posts including: personal opinion on political issues; references to specific bars and restaurants in two German cities; check-ins at gym locations; photos of friends with names tagged; and three threads discussing the subject's then-current employer in critical terms.

The account is discoverable via name search and via the headshot, which matches the subject's current LinkedIn photo. The bio still lists the city of residence as of 2018, which is the same as today.

ANALYST NOTE This is the highest-severity social-media finding. The account exposes personal location patterns, social network, political views, and prior employer criticism — all of which are usable for both targeting (location patterns) and pretext-building (social network names, employer criticism that could be used as a wedge in a social-engineering approach). Recommendation: deletion, not deactivation (action I-3 in §10). Deactivation leaves the data recoverable for 30 days; deletion after the deactivation window is the only durable mitigation.

M-013 MEDIUM **Facebook profile locked but exposes profile picture and friend count**

Subject maintains a private Facebook profile. Account-level privacy is enabled correctly: timeline, friends, photos, and personal information are not visible to unauthenticated viewers. However, the profile picture remains visible (set to public, likely default) and shows the subject with two children whose faces are visible. The profile picture has a creation date of 2023.

ANALYST NOTE Profile-picture visibility is a frequently-overlooked Facebook default. The picture itself is the leak: family composition (two children, approximate ages), the subject's recent appearance (useful for impersonation or pretexting), and the timestamp.

M-014 LOW **Professional association directory exposes biographical paragraph**

A German professional association directory lists the subject with a 280-word biographical paragraph covering career history, qualifications, and one named family connection (a parent's name, included in a context about generational professional continuity). The page is publicly indexed and surfaces on page 2 of the subject's Google trace.

04 · Profile photo reverse image search

Where the subject’s LinkedIn headshot and other published photos appear elsewhere online.

Method

Three reference images were used: the current LinkedIn headshot, an older speaker portrait from a 2022 conference website, and a crowd-photo from a 2019 industry event in which the subject is tagged. Each image was reverse-searched across the four major image-search engines and across facial-recognition-based services where lawful. Cropped variants (face-only, background removed) were also searched to defeat simple hash-based matching.

Findings

M-015 MEDIUM **LinkedIn headshot has propagated to three secondary sites**

The current LinkedIn headshot was located on three additional sites: a former-employer’s alumni-page archive (Wayback Machine, 2019); an industry-event speaker page (live, 2022); and an automatically-scraped business-directory site of unclear legitimacy (live, contact details lifted from public sources). The third site is the most concerning because it presents the subject’s data as if directly furnished by the subject, which it was not.

ANALYST NOTE Auto-aggregated business directories are a known disinformation surface. They can be used as a ‘legitimate’ source by phishers (‘I got your contact from your directory listing’). Recommendation: send a takedown request to the third-site operator citing GDPR Art. 17 right to erasure (action S-7 in §10).

M-016 LOW **Crowd photo from 2019 event identifies subject by name**

The 2019 industry-event photo is hosted on the event organiser’s website with the subject identified by full name in the image caption. Two further attendees in the same photo are also named. The page is indexed and surfaces on page 3 of an image search of the subject’s name.

05 · Dark web & breach database exposure

The subject's historic email addresses checked against documented public breaches and commercial threat-intelligence indices.

Method

Two email addresses were checked: one personal (active since approximately 2002) and one professional (active since 2015). Both were queried against Have I Been Pwned, four commercial breach indices we use under licence, and two specialist credential-stuffing list aggregators. Where a breach was confirmed, we examined whether the password hash was available, whether it had been cracked, and whether the cracked plaintext appears in any current circulation.

What we did not do. Active dark web infiltration — joining forums, contacting vendors, purchasing breach archives — is out of scope for The Mirror. That work is the scope of The Lockdown (see §10, recommendation N-2). Mirror coverage is limited to indices that already aggregate breach data from public and licensed sources.

Confirmed breach exposure

Breach	Scope	Affected address	Hash status	Result
LinkedIn breach 2012	Disclosed 2016, 164M records	Personal email	SHA-1, unsalted	CRACKED — see M-017
Dropbox breach 2012	Disclosed 2016, 68M records	Personal email	bcrypt + SHA-1	Bcrypt portion holds; SHA-1 cracked — see M-018
Adobe breach 2013	153M records	Personal email	3DES (reversible)	Plaintext recovered — see M-019
Collection #1 aggregation	Published 2019, 773M records	Personal email	Cleartext aggregation	Credential pair circulating — see M-020

M-017 HIGH **LinkedIn 2012 — credential pair cracked and circulating**

Personal email m[redacted] appears in the LinkedIn 2012 breach disclosed publicly in May 2016. The associated SHA-1 password hash is present in the breach and has been cracked. The plaintext password follows a discernible pattern: a personally-meaningful word concatenated with a two-digit number.

ANALYST NOTE The plaintext password is not reproduced in this report. Its structure matters: the same structure (word + 2-digit suffix) appears in M-020 (Collection #1). That is the credential-reuse signal. Recommendation: assume any account that ever used a variant of this password is compromised, and rotate. Action I-1 in §10.

M-018 HIGH **Dropbox 2012 — bcrypt portion holds, SHA-1 portion cracked**

The same personal email m[redacted] appears in the Dropbox 2012 breach disclosed in 2016. Dropbox stored hashes in two formats during the migration period: bcrypt (modern) and SHA-1 (legacy). The subject's record contains both; the bcrypt portion has not been cracked, but the SHA-1 portion was, and the recovered plaintext matches the same structural pattern observed in M-017.

ANALYST NOTE The pattern match across two independent breaches is the consequential signal. It confirms the subject reused a password structure across multiple services in this period. Even if the specific plaintexts are now obsolete, the structural insight informs targeted credential stuffing — an adversary can generate variants of the structure with high success probability.

M-019 HIGH **Adobe 2013 — plaintext recovered, password hint leaked**

Personal email m[redacted] appears in the Adobe 2013 breach. Adobe used 3DES with a single shared key, a configuration which made the breach effectively reversible: the plaintexts were recovered en masse within months of the disclosure. Additionally, Adobe stored a password hint field in cleartext alongside the ciphertext. The subject's hint field, while not the password itself, narrows the password search space substantially.

ANALYST NOTE Adobe 2013 is the most thoroughly-cracked breach in the public record. Any password that appeared in it must be considered permanently compromised. The hint field is a separate finding: it should be considered to have permanently revealed information about the subject's memorable-data choices, which may still inform password attempts on other accounts.

M-020 HIGH **Collection #1 — credential pair appears in current circulation**

Collection #1 is a credential-stuffing aggregation published in January 2019 containing 773 million unique email addresses paired with plaintext passwords compiled from multiple prior breaches. The subject's personal email m[redacted] appears in Collection #1 with two distinct paired plaintexts. Both pair plaintexts conform to the structural pattern identified in M-017 and M-018.

Collection #1 has been redistributed through credential-stuffing toolkits since 2019 and the data must be considered permanently in circulation. Any currently-active account using either pair plaintext or a close variant is at high risk of automated takeover.

ANALYST NOTE Recommendation: the subject should treat any account that has used the affected email — whether the current password matches a Collection #1 entry or not — as a candidate for compromise. Priority rotation: financial, email, cloud storage, anywhere multi-factor authentication is not currently enforced. Action I-1 (urgency) and I-4 (MFA) in §10. Further investigation of what is currently circulating about the subject in forum markets and vendor channels is the scope of The Lockdown.

M-021 MEDIUM **Professional email — no breach exposure**

The subject's current professional email [redacted].com was checked against the same set of indices. No breach records were located. **This is a positive finding.** The professional email has not been exposed in any documented public breach to the date of this report.

ANALYST NOTE This is recorded as MEDIUM rather than LOW because the absence of breach exposure does not mean the address is invisible to attackers. The address surfaces in five public sources (see M-003, M-007, and the discussion in §09), and absence from breach indices is not a guarantee of absence from vendor-channel inventories — by definition, those are not in commercial indices yet.

06 · Data broker & people-search assessment

Platforms that assemble and publish personal data scraped from public records, social signals, and commercial sources — without the subject's consent.

Terminology — read this first

People-search platforms are publicly searchable websites that compile profile pages on individuals from aggregated public-records data. Anyone can search them; no commercial relationship is required. Examples relevant to a German subject include [redacted].de, [redacted].com, and a small number of cross-border platforms such as Pipl. These are the surface that matters for the subject's public exposure.

Data brokers are corporate-facing data businesses (Acxiom, Experian Marketing Services, Oracle Data Cloud, LexisNexis Risk Solutions, and similar). Their records are sold or licensed to other companies, not directly viewable by the public. A separate exposure surface — meaningful for marketing profiling and certain investigative scenarios, but not for the typical adversary who would target this subject. Mirror coverage notes broker exposure where indicators surface in people-search records, but does not enumerate broker holdings (out of scope; partial in The Eraser).

Conflating the two is a common error in vendor marketing and in journalism, but they are different categories with different exposure profiles and different remediation paths. We are precise about which is which.

Findings

M-022 HIGH **Two German people-search platforms surface assembled biographical data**

Searches on [redacted].de and [redacted].de return profile pages for the subject containing: full name; current city of residence; age band (presented as a year-of-birth range); two associated relatives (parent and sibling, identified by name); a former employer; and an approximate location at one-postcode-area precision. Each profile assembles this information from a combination of public-records anchor data and commercial enrichment.

Neither platform required the subject to register, opt in, or consent. Both platforms publish the data on URLs indexed by Google: the subject's profile pages appear on page 2 of the name-search Google trace (cross-reference §02).

> **ANALYST NOTE** These are the single highest-leverage findings in the report. People-search platform profiles are the primary input most social engineers will use because they aggregate. An attacker who pulls these two profiles has, in seconds, what would otherwise require 30 minutes of investigation. Recommendation: opt-out under each platform's removal procedure (see Appendix B for instructions specific to these platforms). Removal is achievable but not always durable — many of these sites re-list profiles after a refresh cycle of 60 to 180 days. For durable removal, see The Eraser engagement, which includes monitoring and re-list response.

M-023 MEDIUM **Pipl and one cross-border aggregator return matching records**

Pipl and one further cross-border people-search aggregator return matching records for the subject, drawing in part on the German platforms in M-022 and in part on social-media-derived data. Both records are correctly identified to the subject (no mismatched information). Both can be removed via opt-out procedures.

> **ANALYST NOTE** Cross-border aggregators present a particular problem: removal from the German-language platforms does not remove the data from the international ones, which often refresh from independent sources. Opt-out must be pursued on each platform individually.

06 · The broker landscape (context)

The five platforms that surfaced the subject are a small subset of the broader people-search ecosystem. Across Europe and North America we currently track over 300 platforms in active operation. The remediation challenge is

not removing the subject from the two German platforms above — both have functioning opt-out procedures and the removals can be achieved in a normal Mirror-to-Eraser engagement. The challenge is that **removal is recurring, not one-time**: platforms re-list profiles from refreshed source data, new platforms enter the market, and existing platforms expand their geographic coverage. A single round of opt-outs is necessary but not sufficient.

Currently surfaces subject	5	Two German + Pipl + two cross-border
Likely to surface within 12 months	8–12	Based on overlap with broker-data feeds
Removable via standard opt-out	5	All five currently active findings
Re-list cycle observed	60–180 days	Typical refresh interval per platform
Durable removal effort	Recurring	Quarterly verification recommended

What removal achieves. Pursued for the five platforms above, opt-out reduces the assembled-data exposure to effectively zero on page 1 of the subject's Google trace, and reduces the people-search exposure on pages 2 and 3 substantially. Combined with the recommended Wayback Machine remediation (see M-006), the practical effect is that a casual searcher will find professional content only. An adversary with specialist tooling will still find more, but the cost-to-find rises significantly.

07 · Public records

What was found, what was not, and why the absence of findings here is itself a **jurisdictional protection** the subject benefits from.

HEADLINE FINDING

No exploitable public-records exposure was identified. Under German law, the records that would generate the most acute exposure in other jurisdictions — court filings, address registries, voter rolls, property records — are not publicly searchable. This is not a gap in our investigation. It is a feature of the legal environment that materially limits what an adversary can assemble.

What is closed under German law

Germany applies the principle of informationelle Selbstbestimmung (informational self-determination), established in the 1983 Federal Constitutional Court Census Decision and since strengthened by the GDPR and the federal Bundesdatenschutzgesetz (BDSG). The practical consequence for the subject is that several categories of personal data, which are publicly searchable in many other jurisdictions, are not accessible without a specific legal basis.

Record type	Status	Implication for the subject
Civil court filings	Closed	Court records are not publicly searchable. Selected judgments are published in anonymised form. An adversary cannot retrieve litigation history by name.
Residential address registers (Meldedaten)	Closed by default	Held in municipal registers (Meldebehörden). Disclosure requires either the subject's consent or a specific legal basis under §44/§45 BMG. A general request from a third party with no legal basis will be refused.
Voter rolls	Closed	The electoral register is not a publicly searchable document. There is no equivalent of the publicly-purchasable voter file that exists in some other jurisdictions.
Property and land-ownership records (Grundbuch)	Restricted	Held in the Grundbuch at the local Amtsgericht. Access requires a demonstrable legitimate interest (berechtigtes Interesse). A casual searcher cannot retrieve ownership records by name.
Vehicle registrations	Closed	Held by the Kraftfahrt-Bundesamt. Disclosure requires specific legal basis.
Personal tax records	Closed	Subject to strict tax secrecy under §30 Abgabenordnung.
Marriage / divorce records	Closed	Held in the Standesamt. Disclosure to non-parties requires a legitimate interest.

07 · Public records (continued)

What remains open — and how to read it

Two categories of record are publicly accessible and were checked. Both surfaced data on the subject. Neither rises to a high-severity finding, for the reasons explained below.

Record type	Status	Result for subject
Handelsregister (Commercial Register)	Open	Searchable via the Unternehmensregister portal. The subject does not appear as a director, managing director, or registered shareholder of any German company. **No finding.**
Transparenzregister (Beneficial Ownership)	Restricted since 2022	Following the CJEU ruling in C-37/20 and C-601/20 (November 2022), beneficial-ownership access in the EU is no longer general-public. Access requires demonstrating a legitimate interest. The subject does not appear in publicly-accessible disclosures. **No finding.**

Comparative context — why this matters

We include this comparison because some clients arrive expecting the public-records section to be a major exposure surface, having read about how it works in the United States. The contrast is sharp:

Record type	United States	Germany
Home address	Publicly searchable via county and state assessor records	Closed; municipal register, restricted disclosure
Voter registration	Publicly purchasable in most states	Not public
Court filings	Public via PACER and state systems	Not public
Property ownership	Public county records, name-searchable	Restricted; berechtigtes Interesse required
Vehicle records	Variable by state, often partially public	Not public
Marriage / divorce	Public in most states	Not public

Implication for the subject

A US-resident peer of equivalent seniority would, at minimum, surface a current home address, a property-ownership record (and therefore a purchase price), often a vehicle, and frequently a marriage record naming the spouse and a date — all from public-records searches at zero cost and zero friction. None of this is true for the subject. The German legal environment provides a substantive baseline of protection that should be understood and preserved.

What this means in practice. Two things. First, the exposure that does exist in the subject's footprint (categories 02–06 of this report) accounts for nearly all of the practical targeting surface. The remediation effort focused on those categories will have outsized impact because no public-records surface is feeding back into the exposure. Second, this protection is conditional on the subject remaining within the German jurisdiction. A planned move to the US, the UK, or several other open-records jurisdictions would change the exposure profile substantially. If a relocation is anticipated, a re-audit ahead of the move is recommended (see The Mirror — Re-engagement, or Pre-Transaction Privacy Audit add-on).

M-024 LOW **No public-records exposure surfaced under German law**

No publicly-searchable German records expose the subject's home address, court history, property holdings, vehicle registration, voter registration, or marital status. Commercial-register and beneficial-ownership searches returned no matches. The subject does not appear in any publicly-accessible regulatory disclosure.

ANALYST NOTE Classified LOW (not zero) only because public-records environments are not static. Recommended monitoring: re-check Handelsregister and Transparenzregister annually if the subject takes on a directorship or shareholding; re-audit if jurisdiction changes.

08 · Risk synthesis

How the 23 findings combine into a usable targeting profile, and where the practical exposure concentrates.

The two-hour assembly test

We test exposure by asking: how long would it take a competent OSINT investigator, starting from the subject's full name and nothing else, to assemble a usable targeting profile? For this subject, the answer is approximately two hours — and most of that time is spent on page-2-onward Google results and people-search platforms.

An adversary with two hours of effort would assemble:

Assembled element	Source	Time
Identity confirmation	LinkedIn + professional association directory + page-1 search results	5 minutes
Current city + age band	People-search platform (M-022)	5 minutes
Two named family members	People-search platform (M-022) cross-referenced with M-002 (gaming friends list)	10 minutes
Personal email address	Legacy forum (M-001) + Wayback Machine alumni page (M-006)	20 minutes
Working credential pair candidate	Collection #1 lookup (M-020) + password-pattern analysis (M-017, M-018, M-019)	30 minutes
Personal location patterns + social network	Old Twitter account (M-012) + check-ins + tagged friends	40 minutes
Recent family appearance (faces)	Facebook profile picture (M-013) — visible despite locked profile	5 minutes
Pretext anchor for social engineering	Combination of the above — prior employer criticism (M-012) + family awareness (M-013)	5 minutes

Where the exposure concentrates

Three categories carry the practical risk:

Old credentials. Four documented breaches, a recovered password pattern, and confirmed circulation of credential pairs in a public aggregation. The risk is automated credential stuffing against any account that has ever used a variant of the subject's historic password structure — particularly any account without multi-factor authentication.

People-search platform aggregation. Two German platforms publish an assembled biographical profile including family connections, current city, and age band. The risk is twofold: the data is immediately available to any motivated researcher, and the family connection data extends the exposure surface to people who have not consented to be associated with the subject's public role.

Old social-media accounts. Specifically the 2010–2018 Twitter account, which leaks personal location patterns, social network, opinion content, and an employer-criticism thread that an experienced social engineer would use as a pretext anchor.

09 · Prioritised action plan

What to do, in what order, by when. Three horizons: immediate (within 7 days), short-term (within 30 days), long-term (ongoing).

Immediate — within 7 days

Four actions. All address the highest-severity findings.

ID	Action	What and why	From finding
I-1	**Rotate all credentials that match the recovered pattern**	Any account currently using a password matching the structural pattern recovered from M-017, M-018, M-019, or M-020 must be rotated. Priority order: email accounts (especially the personal address that appears in the breaches), financial services, cloud storage, password manager (if any), social media. Use a password manager to generate new credentials per account — no reuse, no pattern.	M-017 to M-020
I-2	**Delete or rename the legacy forum account**	The forum account identified in M-001 is the single most consequential identity bridge in the report. Either delete the account (preferred) or, if deletion is not supported by the platform, change the username and remove the linked real-name field.	M-001
I-3	**Delete the dormant Twitter account**	Note: deactivation alone is not sufficient. Twitter (X) retains deactivated account data for 30 days. Deactivate, then return after 30 days to verify deletion has completed.	M-012
I-4	**Enable multi-factor authentication on all accounts using the affected email**	Any account where the personal email in M-017–M-020 was used as the login identifier must have MFA enabled. Preference order: hardware security key, app-based TOTP, SMS as last resort.	M-017 to M-020

Short-term — within 30 days

Eight actions. These address the people-search exposure, the residual social-media exposure, and the secondary identity-bridging risks.

ID	Action	What and why	From finding
S-1	**Opt-out from both German people-search platforms**	Each platform has a removal procedure. See Appendix B for current procedures. Verify removal at T+30 days and again at T+90.	M-022
S-2	**Opt-out from Pipl and the second cross-border aggregator**	Each via the platform's opt-out procedure. Removal is generally honoured but must be requested per platform.	M-023
S-3	**Update or delete the Xing profile**	If the subject does not actively use Xing, delete the account. If retained, update to current role only and remove the older photo.	M-011

ID	Action	What and why	From finding
S-4	**Change the public profile photo on Facebook**	If retention of the current photo is meaningful, set the profile picture to a non-personal image and use a current photo only for in-platform display where privacy is enforced.	M-013
S-5	**Rewrite the code-repository commit history email**	Use the platform's rewrite-email feature to redact the historic professional email from commits, or make the profile private if commit content is not needed publicly.	M-003
S-6	**Delete the dormant gaming platform account**	Including verification that the friends list visibility is removed.	M-002
S-7	**Send a GDPR Art. 17 erasure request to the unauthorised business-directory site**	Template language available in Appendix C.	M-015
S-8	**Request Wayback Machine removal of the three most consequential archived pages**	Specifically: the 2009 alumni page with the contact email, the 2013 directory page with the employer, and the 2016 conference programme with the personal mobile.	M-006

09 · Action plan (continued)

Long-term — ongoing

Five practices. These are recurring rather than one-time. They maintain the exposure reduction the immediate and short-term actions achieve.

ID	Action	What and why	From finding
L-1	**Quarterly people-search re-check**	People-search platforms re-list on refresh cycles of 60–180 days. A quarterly verification — running the same searches across the same platforms — surfaces re-listings before they propagate. This is the work the Eraser engagement performs as a standing service.	M-022, M-023
L-2	**Annual breach-database re-check**	Use Have I Been Pwned's notification feature for the personal email going forward. Re-check the professional email manually once per year. Any new breach involving an active credential pair is an immediate-action item.	M-017 to M-021
L-3	**Use email aliases for new accounts**	For any new online account that is not strictly necessary, use a generated alias (services such as SimpleLogin or Apple Hide My Email). This prevents the primary email from accumulating breach exposure as services are breached over time.	Methodology
L-4	**Treat the LinkedIn presence as the public face**	The LinkedIn profile is currently well-managed and is the appropriate professional surface. The discipline is to keep personal content off it and off platforms linked from it.	M-010
L-5	**Re-audit ahead of any jurisdictional change**	A move to the US, UK, or another open-records jurisdiction will substantially expand the public-records exposure surface. Re-audit ahead of the move and pursue available pre-move remediation.	M-024

Summary — what reduction looks like in 30 days

If the immediate and short-term actions above are completed, the two-hour assembly test described in §08 changes materially. The credential pair candidate is no longer useful (rotation closes it). The people-search assembly returns no profile on the subject for the next 60–180 days (until the next platform refresh cycle, addressed by L-1). The Twitter account is gone and cannot be retrieved from the live web (though archive copies may persist). The forum identity bridge is broken. An adversary repeating the same exercise in 30 days would, in the same two hours, assemble considerably less: the LinkedIn presence, the professional directory, and the Facebook profile picture would remain, but the family-naming, the credential candidate, and the historic location patterns would not.

10 · What this report does not cover

Mirror is foundational, not exhaustive. The findings above set the boundary; here is what falls outside it.

The Mirror is the first engagement type for most clients because it answers the question what is currently findable? Several adjacent questions are outside its scope but, depending on the findings above, may now be relevant. Three are listed below. Mirror findings carry forward into each — no investigation is repeated.

The Lockdown — €995 fixed

What is currently circulating in vendor channels and forum markets — beyond the breach indices Mirror queries

Relevant in this engagement: yes — see M-020 (Collection #1) and the note in §05 on the limit of index-only coverage. The Lockdown investigates active circulation, which Mirror by design does not.

The Eraser — €3,800 fixed

Active manual removal across 150+ data brokers and people-search platforms, with 90-day re-scrub monitoring

Relevant in this engagement: yes — see M-022, M-023, and L-1. Mirror identified the exposure and described the remediation; the Eraser performs the recurring remediation work.

The Shield — from €2,200

Structured threat investigation — adversary profiling, harassment patterns, impersonation response

Relevant in this engagement: no current indicator. The findings here describe an exposure surface, not an active threat pattern. The Shield is the right engagement if an active adversary is identified.

How to proceed

The Mirror engagement is now complete. The subject has 30 days of follow-up access to ask questions about any finding in this report. Any subsequent engagement carries this report's findings forward at no additional investigation cost — the work above is the foundation, not a re-billable artefact.

Contact: enquiries@privacyinsightsolutions.com · privacyinsightsolutions.com/contact

Appendix

Methodology sources, data-handling, and reference notes.

A.1 · Source categories

The Mirror investigation draws on the following source categories. Specific tools and platforms are not named in client deliverables; this is a deliberate methodology-protection choice and is consistent across all engagements.

Search engines	Major search engines, image search, archived pages (Wayback Machine)
Breach indices	Have I Been Pwned + four commercial breach indices under licence
Username discovery	A standard set of 312 platforms covering social, gaming, code, marketplace, photo
People-search platforms	German and cross-border platforms; manual querying, no scraping
Public registers	Handelsregister, Unternehmensregister, Transparenzregister (DE)
Reverse image search	Major image-search services + lawful facial-recognition cross-checks
Forum and archive	Wayback Machine, Google cache, specialist archive services

A.2 · Jurisdictional limits

Public-records access varies by jurisdiction. For this subject, the relevant constraint is the German legal environment described in §07: civil court filings, residential address registers, voter rolls, property records, vehicle registrations, and tax records are not publicly searchable and were not investigated. This is the boundary of lawful Mirror practice in this jurisdiction, not a methodology gap.

A.3 · Data handling

All raw investigative data — including search artefacts, queries, intermediate notes, and source captures — is held only for the duration of the engagement and the 30-day follow-up window. At the end of that window, raw data is purged in accordance with the published Data Purge Policy at privacyinsightsolutions.com/data-purge-policy.

The delivered PDF report is retained by the client. PI Solutions retains a hashed engagement record (no personal data) for accounting and methodology-improvement purposes only.

A.4 · Ethics

Every Mirror engagement operates under the published Ethics Code at privacyinsightsolutions.com/ethics-code. The core commitments relevant to this engagement: first-party consent only (the subject is the client); lawful OSINT methods only; no impersonation, no social engineering of third parties, no unauthorised access to systems; analyst-pair verification on every finding before inclusion.

A.5 · About PI Solutions

Privacy Insight Solutions is a human-led OSINT investigation and digital privacy management firm. We work with executives, high-net-worth individuals, and organisations whose privacy is a professional requirement. The firm is based in the Netherlands and operates by appointment. We do not name clients, publish testimonials, or use case studies. Discretion is not a marketing claim; it is the operating principle.

END OF SAMPLE REPORT · PI. SOLUTIONS · DISCRETION BY DESIGN