Sound of da Police:

Responding to Law Enforcement Data Requests

European Privacy KnowledgeNet 2026 · Munich · 12 October 2026

Dr. Isabelle Brams · Kai Traubinger

EXTERNAL COUNSEL × IN-HOUSE PERSPECTIVE

Today’s speakers



Dr. Isabelle Brams

Associate · Latham & Watkins
Litigation / GDPR defense / EU Data Law



Kai Traubinger

Senior Data Protection Manager · zooplus
In-house process / privacy operations

OPENING PREMISE

The request looks simple.

An authority asks for data.
The company has the data.
So the company provides it.

In practice, every request triggers a chain of decisions:

- Who is asking?
- Under what power?
- Are we required or permitted to disclose?
- Which exact data are covered?
- How do we document the call?

Monday, 09:07

Inbox · Customer Care

From: police.department@example.de
Subject: URGENT – Request for customer information

We are investigating online credit-card fraud. Please provide all available information relating to customer account C-18492 within 24 hours, including account details, addresses, orders, payment information and IP addresses.

Legal basis: § 163 StPO

Question for the room: what happens next?

Fictionalised training scenario. Not legal advice.

STORYLINE

We will follow five decisions

1
The Knock
How does the request enter a controlled process?

2
The Power
Can they ask — and do we have to answer?

3
The Data
What exactly is covered?

4
The Pressure
What changes when it gets messy?

5
The Playbook
How do we turn law into process?

One evolving scenario. Four legal mechanisms. One practical framework.

Before the legal analysis: control the intake



Operational point: if the request never reaches the right place, the legal analysis never happens.

Two doors, not one

Door 1

Can the authority obtain the data?

power to request / collect

Legal basis: StPO



Door 2

Can / must the company disclose it?

basis or obligation to transmit

Legal basis: GDPR, TDDDG

Authority to ask ≠ basis to disclose

Authorities: BVerfG, 24.01.2012 – 1 BvR 1299/05; BVerfG, 27.05.2020 – 1 BvR 1873/13, 1 BvR 2618/13.

Request ≠ order

“Please provide…”

General investigative request
§§ 161 / 163 StPO

→ may support a request
→ not automatically a private-company disclosure duty
→ company: Art. 6(1)(f) GDPR + § 24(1) No. 1 BDSG – balance and document

“You are required…”

Production / surrender obligation
§§ 94 / 95 StPO

→ specific legal mechanism
→ stronger route to Art. 6(1)(c) GDPR analysis
→ company: Art. 6(1)(c) GDPR

First classify the document. Then classify the data.

Authorities: BVerfG, 17.02.2009 – 2 BvR 1372/07; BGH, 20.02.2019 – StB 51/18; §§ 94, 95, 161, 163 StPO.

This is not theory – see Hamburg DPA case (2023)

Police request

Drohbriefe investigation. Police requested tenant data from a private property manager for handwriting comparison.

Company response

No automatic disclosure. The company asked for context, legal basis and purpose — then documented the disclosure.

Key point

§161 StPO on authority side
≠
company's disclosure basis

Practical message: ask, clarify, document — without defaulting to "no".

Authority: HmbBfDI, Tätigkeitsbericht Datenschutz 2023, section 14 "Weitergabe von Mieterdaten an die Polizei" (§ 24(1)(1) BDSG).

ACT 3 · The Data

“All customer data” is not a legal category

Name | Email | Phone | Billing address | Delivery address

Order history | Payment info | IP / login data | Customer service | Fraud flags

The legal assessment eventually becomes a data-scoping exercise.

Same person · same investigation · different data · different legal analysis

AUDIENCE MOMENT

By show of hands...

The authority asks for:

> **“all available information relating to the account”**

1. **Who would send the full export?**
2. **Who would send only identity / account data?**
3. **Who would ask the authority to narrow the scope first?**

They know the account. Now they want to know who — and how.

Subscriber / account identity

“Who is behind this account?”

Examples: name, account email, phone, billing address — depending on scope and service.

§100j StPO ↔ §22 TDDDG

Usage / behaviour

“How was the service used?”

Examples: IP / login events, time, duration, extent of use — not automatically covered by subscriber-data logic.

§100k StPO ↔ §24 TDDDG

One customer profile can contain data governed by different disclosure regimes.

Authorities: §§ 100j, 100k StPO; §§ 22, 24 TDDDG; OLG Schleswig, 23.03.2022 – 9 Wx 23/21; OLG Bamberg, 17.12.2024 – 6 W 12/24 e.

Gatekeeper — not prosecutor

Not a mailbox

Formal checks, responsible person, documentation.

→

Company

checks the request
scopes the data
responds within the lawful frame

→

Not the prosecutor

Does not re-run the investigation or create an investigative product.

The hard line is not always "yes" or "no" — often it is "what exactly, under which mechanism?"

Authorities: LG Hannover, 05.08.2026 – 46 Qs 32/26; BGH, 20.08.2015 – StB 7/15; OLG Stuttgart, 19.05.2021 – 2 Ws 75/21.

Pressure changes behaviour. It does not create a legal basis.

URGENT
deadline pressure

SERIOUS CRIME
moral pressure

OFFICIAL LOGO
authority pressure

DO NOT INFORM
confidentiality pressure

Preserve, don't delete (Art. 17(3)(e), 18 GDPR). "Do not inform" needs a statutory exception (Art. 23 GDPR, §§ 32–34 BDSG) or a formal confidentiality order – document why and for how long.

Good process is built for the uncomfortable case — not only for the easy one.

Authorities: BGH, 20.02.2019 – StB 51/18; HmbBfDI, TB Datenschutz 2023, section 14; §§ 22, 24 TDDDG.

And then the request crosses borders

Since 18 August 2026, the EU E-Evidence framework adds a direct cross-border route for electronic evidence.

European Production Order

disclose electronic evidence

default: 10 days

Emergency case

production clock accelerates

as little as 8 hours

European Preservation Order

freeze data before production

preserve before disclose

Narrow grounds for refusal · designated establishment / legal representative · requests from non-EU authorities: Art. 48 GDPR

Operational readiness becomes part of legal compliance.

Sources: Regulation (EU) 2023/1543; Directive (EU) 2023/1544; EBewMG; new §§ 13a, 24a TDDDG.

A practical response framework

VERIFY	Who is asking?
ASSESS	Which legal mechanism?
SCOPE	Which exact data?
RESPOND	Preserve first – then disclose, clarify or refuse?
DOCUMENT	Can we justify it later?

Takeaway

Cooperate.
But know why, what and how you disclose.

What should you remember on Monday morning?

1. The logo at the top is not the legal basis.
2. Authority to ask ≠ basis to disclose.
3. Request ≠ binding production order.
4. Changing the data category can change the law.

The difficult part is not finding the data. It is being able to justify each piece you decide to hand over.

FOR THE PUBLISHED DECK

Sources & further reading

Cases

- BVerfG, 24.01.2012 – 1 BvR 1299/05 (Bestandsdatenauskunft I)
- BVerfG, 27.05.2020 – 1 BvR 1873/13, 1 BvR 2618/13 (Bestandsdatenauskunft II)
- BVerfG, 17.02.2009 – 2 BvR 1372/07 (Operation Mikado)
- BGH, 20.02.2019 – StB 51/18 (post data / serious crime)
- BGH, 20.08.2015 – StB 7/15 (provider not investigator)
- OLG Stuttgart, 19.05.2021 – 2 Ws 75/21 (provider assistance limits)
- BVerfG, 27.06.2018 – 2 BvR 1405/17 (Jones Day / internal investigations)

Authorities & regimes

- HmbBfDI, Tätigkeitsbericht Datenschutz 2023, section 14
- OLG Schleswig, 23.03.2022 – 9 Wx 23/21 (IP as usage data)
- OLG Bamberg, 17.12.2024 – 6 W 12/24 e (Bestandsdaten vs Nutzungsdaten)
- LG Hannover, 05.08.2026 – 46 Qs 32/26 (§ 100j StPO / platform complaint)
- Regulation (EU) 2023/1543; Directive (EU) 2023/1544; EBewMG
- EDPB Guidelines 02/2024 on Art. 48 GDPR (third-country requests)
- Art. 2(2)(d), 6, 23 GDPR; §§ 24, 32–34 BDSG; Directive (EU) 2016/680

Questions?

Thank you.

Dr. Isabelle Brams · Kai Traubinger

#KnowledgeNet #IAPP #PrivacyPro