WHITEPAPER · HES CONSULTANCY INTERNATIONAL

HES CONSULTANCY INTERNATIONAL

YOUR BUSINESS, MY SERVICES

ARE YOU MORE CATHOLIC THAN THE POPE?

What EU & US sales can and can't do with AI-agents, e-mail, enrichment, tracking, and retargeting.

Follow-up to *The Perfect Storm*

AUTHOR | MIKE HES

DATE | NOVEMBER 2, 2026

WHITEPAPER · HES CONSULTANCY INTERNATIONAL

Are you more Catholic than the Pope?

What vendors in Europe and the Netherlands can and cannot do with AI agents, email, enrichment, tracking and retargeting.

Sequel to The Perfect Storm

AUTHOR	Mike Hes
REFERENCE DATE	2 November 2026
AUDIENCE	CxO, CISO, CMO and sales leadership · software vendors and EU partners
REGION	EU / Netherlands, compared with the United States
STATUS	Final version, November 2026

THIS IS NOT LEGAL ADVICE

This document is intended for information purposes. It translates laws and regulations into design and sales choices but does not replace legal advice on a particular campaign, data flow or contractual arrangement.

Foreword — Mike Hes

In more than thirty years in the European ICT sector, I have seen many sales models come and go. First everything revolved around the telephone, then email, marketing automation, social selling and intent data. Now AI is being added to everything. Technology changes. One question remains the same: does this genuinely help the customer, or does it mainly help the seller push harder?

In The Perfect Storm, I described what is changing for organisations: new European rules, greater responsibility at board level and an increasing need to provide evidence. This whitepaper looks at the other side of the table. What can a vendor or partner actually do to approach an organization?

The answer is less black and white than LinkedIn discussions sometimes suggest. 'Cold outreach is dead' sounds modern, but an American playbook using pixels, retargeting, lookalikes and automated nurturing can still take precisely the wrong turn in Europe. Conversely, you can impose such strict rules on yourself that fear prevents you from doing anything, even though the law does allow ordinary commercial communication, provided you distinguish the lawful basis, the channel and the recipient's reasonable expectations.

ALL THAT GLITTERS

My principle is the same as in The Perfect Storm: look beyond the label. “AI”, “outside-in” and “privacy-first” are not evidence. The question is what happens technically, which data you use, which channel you choose, and whether the individual could reasonably have expected it.

For HCI, outside-in is therefore not a marketing term. The interested party — the buying side — receives information, whitepapers, a scan or an assessment and sets the pace. Signals begin at organisational level wherever possible. Once an individual identifies themselves, the use of their data must be clear. And when the next step is commercial, it must make sense both legally and from a human perspective.

This whitepaper offers no trick for circumventing the GDPR. Nor does it prohibit modern sales. It seeks to make the boundary visible. After all, if you know where the boundary lies, you need not be more Catholic than the Pope — and need not cross it inadvertently either.

A decisionmaker receives an average of 117 emails and 153 chat messages per working day and is interrupted approximately every two minutes by a notification, email or meeting [C42]. That does not even include the telephone, social media, television advertising and roadside adverts. Attention has become the scarce resource. Look back at yesterday and you will find that things were left undone. It is no coincidence that two in three business buyers now prefer to purchase without a sales representative [C43].

That is why control must return to the individual. You decide your priorities and what matters to you. Not the caller trying to arrange an appointment because you appeared in a database. Not the salesperson with a perfectly good story on a subject outside your top twenty priorities. Nor the incumbent supplier keen to see you at yet another round-table event. The legislator now recognises this too: since 1 July 2026, businesses may call consumers and self-employed sole traders only where they have given prior consent [C40].

Over more than thirty years in European ICT, I have seen this change of direction. The pandemic accelerated it: decision-makers research matters for themselves, at a time of their choosing. The figures support this. The proportion of business buyers who prefer purchasing without a salesperson rose from 61 to 67 per cent in one

year [C43]. Those who do seek a salesperson increasingly do so to validate what they have already researched themselves, including with AI [C44]. The question is not whether your way of working must change. It is: are you already working this way?

Mike Hes (founder)
HES Consultancy International
Arnhem, 2 November 2026

Who is HCI

HES Consultancy International (HCI) is an independent European ICT consultancy, founded by Mike Hes, with over thirty years of experience in the European ICT sector. HCI advises on strategy and architecture and builds the technology that goes with it.

HCI works outside-in: the buying organisation sets the pace, receives value first — information, a scan or an assessment — and shares data only when there is a concrete reason to. What counts is not the label “AI” or “privacy-first”, but what technically happens, which data is used, and whether the individual could reasonably have expected it. This whitepaper comes directly out of that practice.

https://hes-consultancy.nl/media/video3-en.mp4 (English video)

What HCI offers

HCI helps organisations become visible and find customers responsibly, without crossing the line. In brief, the offering:

- Scans and assessments — free security and compliance scans that show where you stand on visibility, test coverage, follow-up and demonstrability, with a report, no registration or obligations.
- Advice and architecture — outside-in go-to-market, consent flows, data model and channel design that keep GDPR bases and channel rules properly separate.
- AI governance — the HCI AI Gateway with its personal-data filter, audit and role demarcation, so AI agents act only within a boundary set by people and technology.
- Nxt Era — the invitation-based platform that connects supply and demand through a double yes, free for using organisations.
- Nxt Era Solutions is the brand name for products developed in-house, such as: Observator, DealFlow CRM, AI Gateway for PII Filtering (EU vs. US), CMS App, Enrichment App, 360 App, Onboarding App, Campaign App, Contract Builder, and AI Agents Studio.

Want to know where your organisation stands? Start with a free scan at hes-consultancy-international.com.

The essentials up front

This whitepaper is not a plea to push the boundaries, but to know where they really lie — so you need not be holier than the pope, nor cross the line by accident.

Too strict is: forbidding every commercial interest and basing everything on consent alone. The GDPR recognises more legal bases and the Dutch Telecommunications Act has exceptions; inbound, existing customer relationships, purpose-bound B2B contact details and non-personal organisational signals offer real room.

Too broad is: copying a US funnel and assuming one lead magnet covers all follow-up, that a pixel “from the platform” falls outside your responsibility, that a LinkedIn connection is email consent, or that an AI agent may infer the legal assessment from probability.

The sustainable route lies in between: let the buyer see value first, collect personal data only when there is a concrete reason, make purposes visible, keep evidence, keep channel rules separate from GDPR bases, let an AI agent act only within a boundary set in advance, and always give an easy way back.

The HCI position in one sentence: outside-in means not only that the customer sets the pace, but also that you can demonstrate that pace in your data model, your consent flow and your agents.

The checklist: is this allowed?

This is not legal advice. Ten practical situations; exceptions require a case-specific assessment.

1	Commercial email to a LinkedIn contact without consent	**NOT ALLOWED**	Except where the existing-customer exception or an expressly designated business address applies. [B01][C37]
2	Report and follow-up after a scan with a separate marketing opt-in	**ALLOWED**	Separate choices for the report and marketing; retain evidence. [B07][B01]
3	Email an existing customer about your own similar service	**CONDITIONAL**	Details obtained through a sale; provide an opt-out in each email. [B01][B28]
4	Call the general business number of a limited company (bv)	**ALLOWED**	Sole traders and private telephone numbers: prior consent required since 1 July 2026. [C40]
5	Email a purchased or scraped list	**NOT ALLOWED**	No demonstrated channel basis; missing GDPR lawful basis or information obligation. [B01][B08][C50]
6	Activate a marketing pixel before the cookie choice	**NOT ALLOWED**	Obtain consent first; distinguish strictly necessary technology. [B02][B04][B13]
7	Upload a CRM list for custom audiences or lookalikes	**CONDITIONAL**	Assess lawful basis, notice, shared responsibility and transfers. [B08][B15]
8	Connect private email, diary or Drive to an AI tool for sales	**NOT ALLOWED**	In practice: use a business account, processing agreement, bounded sources and documented purpose. [C33][C34]
9	Let an AI agent email or chat with a prospect	**CONDITIONAL**	Valid channel basis; AI disclosure where required by AI Act Article 50; human escalation. [B18][B01]
10	Warm introduction after the introducer first sought agreement	**ALLOWED**	Record who asked, when and for what purpose. [B07]

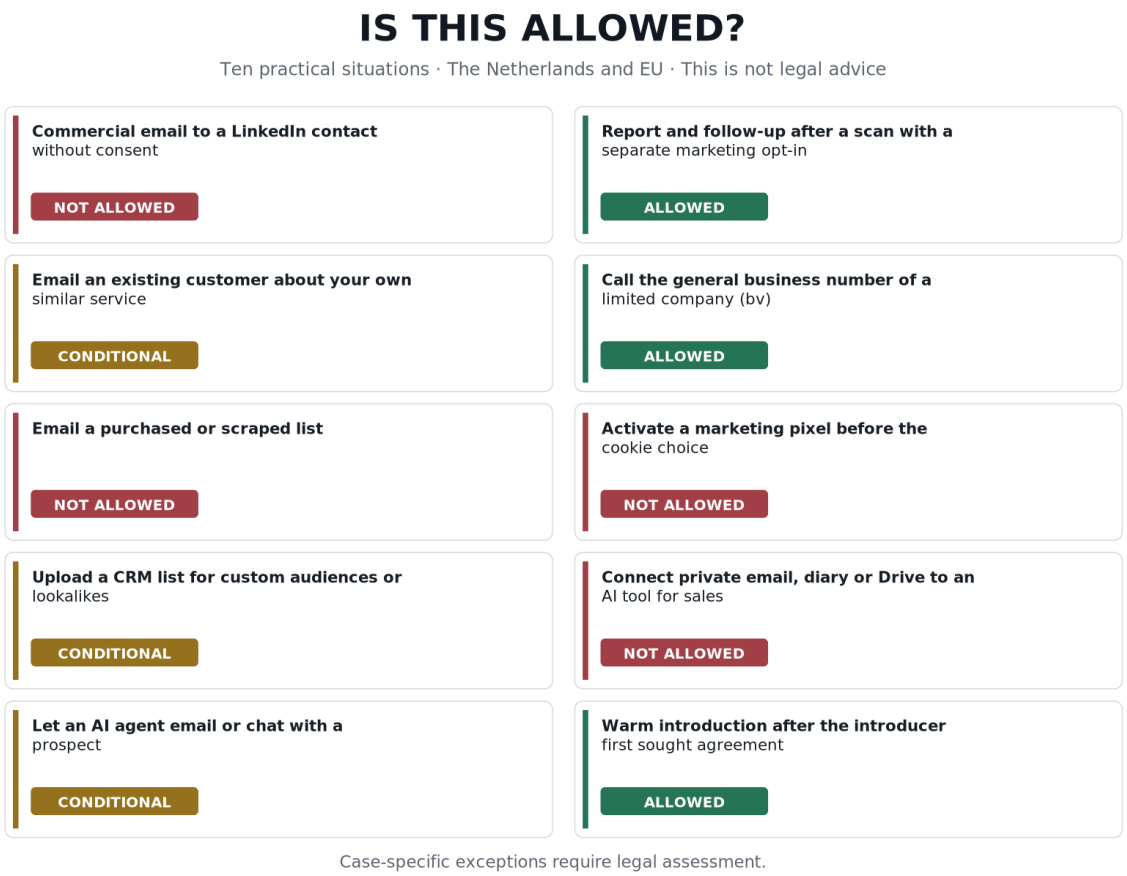


Figure 8. Is this allowed? Ten practical situations. Not legal advice; exceptions require case-specific assessment.

Nxt Era in brief

Many small business owners have no database of their own and do not want to buy one. Nxt Era is HCI's answer: an invitation-based platform where organisations post their own signals — "I'm looking" or "I'm offering" — and set sector, topic and duration themselves.

An introduction only arises from mutual interest: name and email address are exchanged only after a double yes, never through invisible behaviour. No AI on participants' data, only necessary cookies, hosting in Germany, and free for using organisations. That way even a start-up gains access to real demand, without a purchased list as its foundation.

https://hes-consultancy.nl/media/nxt_era_pilot_how_it.mp4 (explains the Nxt Era platform: Nxt Era is a European network for decision-makers and buyers. You post a signal: what you are looking for, and until when. Contact details are only shared after a double yes. No cold outreach.)

1 The essentials in seven rules

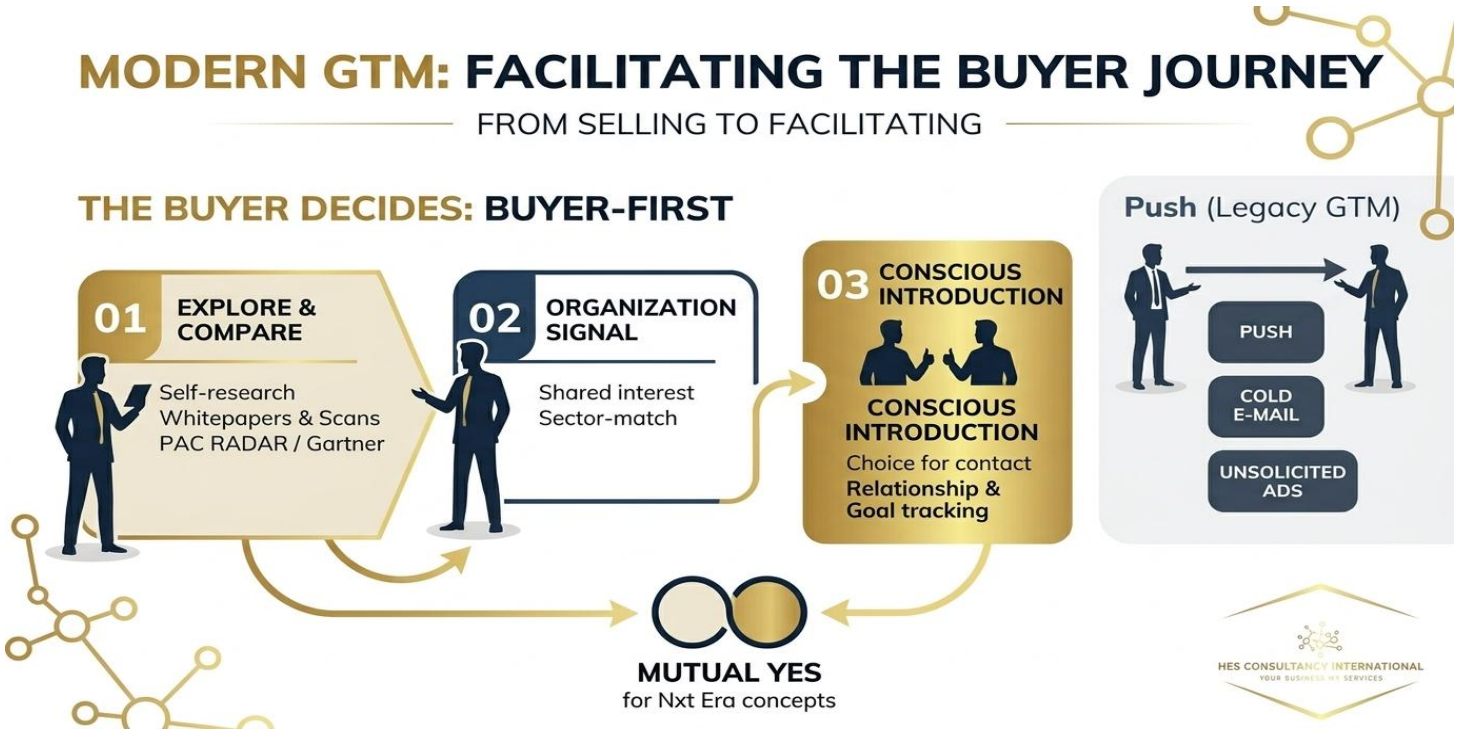
The legal mistake most often made in sales and marketing is to combine three different questions into one debate: may I process personal data, may I use this communication channel, and may I have AI perform this interaction? Different rules apply to each question, and the answers may differ.

Rule	Practical meaning
1. A lawful basis is not channel consent	A legitimate interest under the GDPR does not automatically permit an unsolicited commercial email. Electronic marketing is also governed by the Dutch Telecommunications Act and ePrivacy. [B01][B03][B05][B06]
2. Personal does not mean requested	A handwritten one-to-one email may still be unsolicited commercial communication. Its personal tone does not change the rules for the channel. [B01]
3. B2B is not a blanket exemption	The Dutch B2B exception is narrow: the recipient must have designated and published the contact details for receiving such unsolicited communications, and your use must remain within that purpose. [B01]
4. Pixels are not invisible analytics	Storing or reading information on a device generally requires consent, subject to narrow exceptions. Tracking and retargeting also involve responsibilities under the GDPR. [B02][B04][B13][B14][B15]
5. Public does not mean free to use	Scraping or enriching personal information is still processing. You need a lawful basis, transparency and appropriate safeguards. [B06][B08][B16]
6. An AI agent is also a channel and data flow	An autonomous sales bot may trigger AI Act transparency as well as GDPR and ePrivacy obligations. Processors and subprocessors form a separate contractual chain. [B11][B18][B19]
7. Outside-in works best when built into technology	Make anonymous and organisational-level data the default, explicitly mark the transition to individual-level data, let buyers set the pace, and retain evidence of consent, objections and sources.

THE DECISION RULE

For every campaign, ask these questions in order: 1) What data? 2) What lawful basis? 3) Which channel or device access? 4) Which AI or automation? 5) What evidence and right to object?

02 Changing buyer behaviour: outside-in without magical numbers



FROM PRACTICE

In my conversations with decision-makers over the past five years, I kept hearing the same thing: their way of working had changed, and the pandemic had accelerated it. They research independently first, often through analysts such as Gartner. For many buyers, if you are not in a Magic Quadrant or Hype Cycle, you scarcely exist. European alternatives do exist, including PAC RADAR and Whitelane Research sourcing studies for the Benelux and Nordic countries. But they are less well known, even among European buyers. People increasingly prefer a video call to an office visit, and unfamiliar telephone numbers are less likely to be answered. [C45]

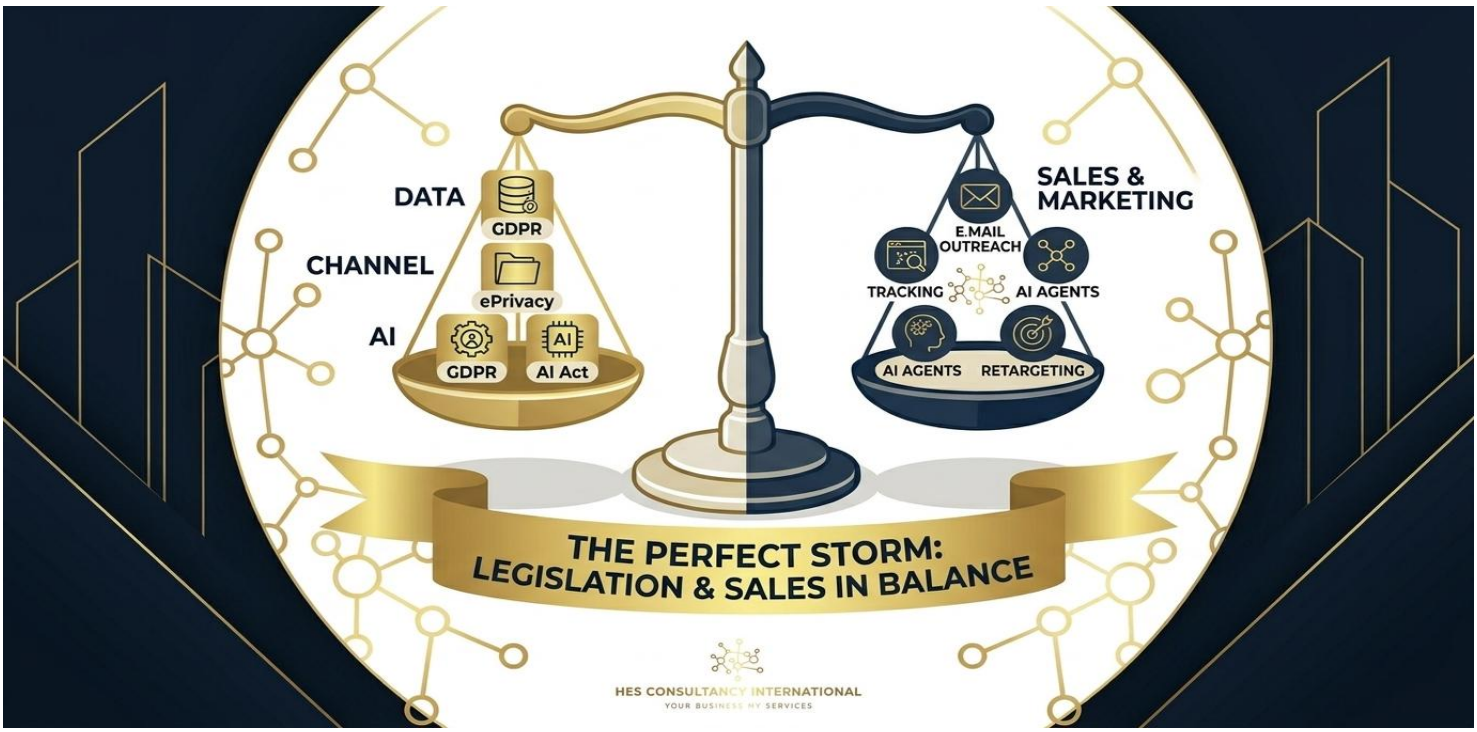
HCI starts from a simple principle: buyers want to research, compare and decide for themselves when a conversation would be useful. Whitepapers, scans and assessments can provide that space. This is a commercial design choice, not a legal loophole.

In B2B sales, people often speak of an increasing number of contact points. Yet there is no reliable market-wide figure, such as '30–40 touchpoints'. The useful observation is qualitative: digital research, multiple stakeholders and longer decision-making processes make the timing and relevance of contact more important.

The public American playbook provided for comparison follows the same commercial direction: first a free resource, then a landing page, advertising, retargeting and automated follow-up. It calls this 'attract, don't chase'. The legal question starts with the technical implementation: which identifier is placed, which list is uploaded, what consent was requested, and who sends which message afterwards? [B29] This also raises the question of which source was used — for example, an American provider holding person X's email address or telephone number.

That is the difference between outside-in as a tone of voice and outside-in as a data model. You can write politely while profiling people invisibly. Or you can store much less personal data, use information at organisational level, and move to individual-level data only when someone consciously chooses to take that step. The latter approach fits the HCI philosophy better and also reduces part of the legal exposure.

03 The legal stack: data, channel and AI



Layer 1 — May you process personal data?

The GDPR requires a lawful basis for every processing operation. Consent is sometimes appropriate for commercial processing, but legitimate interests may also provide a valid lawful basis. In 2024, the Court of Justice confirmed that a commercial interest is not categorically excluded from Article 6(1)(f). That does not mean every commercial interest prevails: you must identify a legitimate interest, demonstrate necessity and balance it against the interests and fundamental rights of the data subject. Less intrusive alternatives and reasonable expectations matter. [B06]

For direct marketing, the individual has a strong right to object. Once a person objects to processing for direct marketing, their personal data may no longer be processed for that purpose. That right must be explicitly brought to their attention no later than the first communication. [B09]

Layer 2 — May you use this channel or device?

Specific ePrivacy and Dutch Telecommunications Act rules apply to electronic marketing and access to terminal equipment. Processing may therefore have a defensible basis under the GDPR while sending the email or placing or reading a tracking identifier still requires consent. In Inteligo Media in 2025, the Court made that distinction explicit: where the soft opt-in under Article 13(2) of the ePrivacy Directive is lawfully used, Article 6(1) GDPR is not an additional test for sending the message. Conversely, a prohibited email cannot simply be 'repaired' by invoking legitimate interests. [B03][B05]

Layer 3 — What changes when AI performs the interaction?

The AI Act does not replace the GDPR or ePrivacy rules; it adds another layer. Where an AI system is intended to interact directly with natural persons, it must in principle be designed so that the person is informed they are interacting with AI, unless this is obvious in the circumstances to a reasonably well-informed person. [B18]

Providers and deployers must also take measures to support the development of AI literacy among staff and other people operating the systems. The current text, as amended in 2026, clarifies that a specific individual level need not be guaranteed. [B19]

NOT A SINGLE “CONSENT”

One checkbox does not automatically resolve every layer. Cookie consent is not email consent. Email consent is not a licence to profile. A GDPR lawful basis is not consent to use a retargeting pixel. And knowing someone is not an exception to every channel rule.

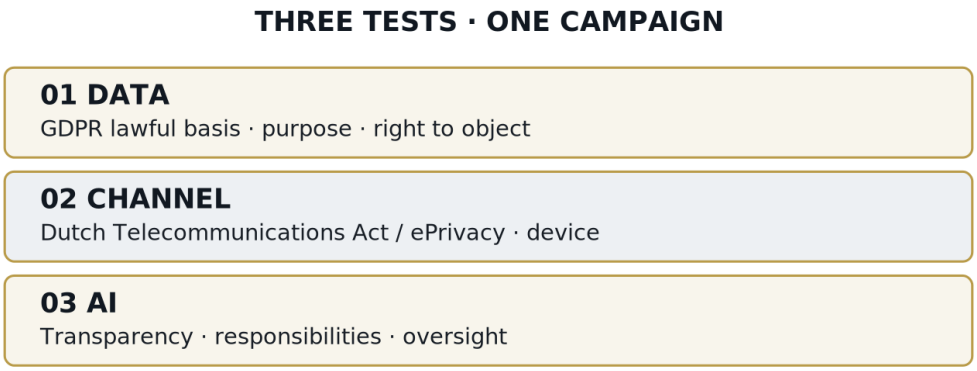


Figure 1. Data, channel and AI are separate tests. [B01][B06][B18]

04 The new reality: nobody knows what they are opening up

What can your AI assistant actually see?

AI helps you manage your diary and email. But when you connected it, did you also grant access to OneDrive or Google Drive? Those may contain photographs of family and friends, the contract for your home or car, and bank statements. At home there is also the smart thermostat, video doorbell and refrigerator that keeps track of groceries. The question is not whether AI is useful, but whether you know what you have opened up. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP) reported incidents where employees entered personal data from, for example, patient and customer files into AI chatbots, potentially exposing it to unauthorised access. [C46]

Today, you do not need a large IT department to give an AI assistant access to a mailbox, calendar, Drive or customer database. A few clicks are enough. You may thereby give a system access to decades of correspondence, documents, invitations and information about people who never chose to participate. That remains true even when the user experiences the tool solely as a convenient sales assistant.

The risk boundary is often crossed unnoticed when private information is put to a business use. Anyone using a private calendar, personal email or private Drive for sales prospecting cannot simply continue to rely on the exemption for purely personal or household activities. That exemption is limited by its nature; for commercial purposes, purpose limitation and a lawful basis must be assessed again. [C33]

A second boundary concerns the agreement with the AI provider. Where that provider processes personal data on the company's behalf, the controller must demonstrably regulate the relationship and instructions under Article 28 GDPR. A consumer service does not automatically provide the same contractual safeguards, access controls and assurances as an enterprise service. The provider's use of data for training and any transfer outside the EEA must also be established on the facts; arrangements differ by provider, product and setting. [C34]

A third boundary concerns the individuals whose data is contained in the connected sources. Where personal data has not been obtained directly from the individual, the information obligation under Article 14 GDPR may arise, subject to applicable exceptions. 'It is in my mailbox' does not answer that question. [C35]

Shadow AI begins with good intentions

The employee wants to reply more quickly, the director wants to serve their network better, and the start-up is looking for affordable support. Nobody sets out to misuse personal data. That is precisely why organisations need to make visible which sources AI systems may access, who approves access rights and for what purpose a connection is used.

Article 4 of the AI Act requires providers and deployers to take measures to support AI literacy among employees and others using AI on their behalf. The obligation is context-dependent: it is not about an identical certificate for everyone, but understanding the opportunities and risks of AI in one's own role. [C36]

Figure 2. Data sources accessible to an AI assistant: illustrative overview. [C33][C34]

Five questions before connecting an agent

- Is this a business or private source, and who controls it?
- Which personal data, including potentially special-category data, will become accessible?
- For what explicit purpose was that information originally collected?
- Which provider will gain access, under what processing arrangements, retention periods and international transfers?
- How can you subsequently prove what the agent retrieved, transmitted or retained?

The answer is not to stop using AI. The answer is not to connect an unrestricted data source before the source, the action and the responsibility are clear.

05 The US playbook examined: where does it conflict with EU/NL rules?

The Aletto report provided is a useful public example of an American growth playbook. Among other things, it recommends offering a free resource in exchange for contact details, an opt-in landing page, paid advertising, lookalike audiences, visitor retargeting and automated email and SMS follow-up. Its revenue, conversion and performance figures are the author's marketing claims and are not presented here as independently established facts. [B29]

Step	US playbook	EU/NL assessment	Practical design
1. Lead magnet / scan	Offer value in return for a name and business email address.	Requesting a resource does not automatically amount to broad consent for all future marketing. Consent must be specific and demonstrable. Soft opt-in may apply within a concrete service relationship; Inteligo shows that even a free service may qualify in some circumstances. [B01][B05][B07]	Separate report delivery from commercial follow-up. When in doubt, provide a separate marketing choice.
2. Paid adverts to a landing page	Advertising drives traffic before the visitor is known.	Contextual or platform-native targeting without your own individual list may be less intrusive than cross-site tracking. The GDPR and ePrivacy rules come into play when personal data or device identifiers are used. [B02][B04][B15]	Start with the least intrusive targeting and measure without unnecessary personal identification.
3. Pixel and retargeting	Approach non-converting visitors again later.	Access to or storage on terminal equipment generally requires prior consent, subject to narrow exceptions. Tracking can create joint controller responsibilities for some processing activities. [B02][B04][B13][B14][B15]	Do not fire marketing pixels before a valid choice. Document roles and purposes.
4. Lookalike / custom audience	Upload your own email or telephone list to match users and build similar audiences.	An upload constitutes processing and transmission to a platform. The EDPB explicitly addresses list-based targeting as processing for which the advertiser and platform may share responsibility. [B06][B08][B15]	Record the source and expectations, choose a suitable lawful basis, enable objections, and assess platform terms and potential international transfers.
5. Nurture email	Automated sequence after a download or registration.	Commercial email is subject to Article 11.7 of the Dutch Telecommunications Act and ePrivacy. Consent is the general rule, with narrow exceptions. Each message must identify the sender and provide a way to stop. [B01][B03][B28]	Make purpose, sender and frequency predictable. Stop immediately on objection.
6. SMS AI bot	Automated reminder or conversation to arrange a meeting.	SMS is an electronic message and the same Dutch consent logic applies. Where the bot interacts directly with an individual, Article 50 AI Act transparency may also apply. [B01][B18]	Ask for channel-specific consent and explain that the interaction is with AI where this is not already obvious.

The striking conclusion is that an American playbook can be commercially outside-in — offer value before selling — while being legally inside-out because the seller has already built a personal profile behind the scenes. The European approach requires these two dimensions to be separated.

06 Email: what is permitted, and when is “personal” misleading?

General rule: prior consent

Article 11.7 of the Dutch Telecommunications Act (Telecommunicatiewet) prohibits the use of electronic messages for unsolicited commercial, charitable or ideological communications unless the sender can demonstrate prior consent. The legislative history expressly mentions email, SMS and WhatsApp. Even an unsolicited electronic message asking only 'may I send you marketing emails in future?' can itself be unsolicited commercial communication. [B01]

B2B exception: much narrower than “the business address is online”

Prior consent is not required for a legal person or someone acting in a professional or business capacity where the sender uses electronic contact details that the recipient has themselves designated and published for receiving such unsolicited commercial, charitable or ideological communications, and the use remains within the stated purpose. A general contact address on a website is therefore not automatically an invitation for every sales message. [B01]

Existing customers: soft opt-in for own similar products or services

A sender who obtained a customer's electronic contact details in connection with the sale of a product or service may, subject to conditions, use those details for its own similar products or services. The customer must be offered a simple, free opportunity to object both when the details are collected and in every message. The amendment effective from 1 July 2026 primarily tightened telemarketing rules; the existing-customer exception for electronic messages remained a separate exception to the general rule. [B01][B28]

Someone you know or a LinkedIn connection

A demonstrable relationship may be relevant to the GDPR balancing exercise: someone may reasonably expect particular data processing where a genuine context or relationship exists. But that does not automatically permit a new commercial email under Article 11.7. The safer question is therefore not 'do I know them?' but 'was this message requested, does it demonstrably fall within a statutory exception, or do I have valid consent?' [B01][B06]

FOR HCI

The rule of thumb “a personal one-to-one email to someone you know is allowed” is too broad as a statement of law. It can remain a commercial code of conduct, but it must always include the Article 11.7 channel check. This prevents evidence of a relationship from being confused with consent.

Figure 3. Decision tree for commercial email; exceptions require case-specific assessment. [B01][B28]

Download or scan: one form, two purposes

When someone enters their information to receive a scan report, the initial processing is needed to provide the requested service. That is not the same as consent to a nurturing sequence. Marketing consent must be freely given, specific, informed, unambiguous and demonstrable. At the same time, Inteligo shows that a free online service can, in specific circumstances, fall within the ePrivacy soft opt-in. 'Free means never a customer' is therefore not a safe general rule either. [B05][B07]

For an HCI-style scan, a separate, understandable marketing choice is the most robust operational approach: 'send me the report' is one purpose; 'keep me informed by email about similar analyses or solutions' is another. The second choice can then be retained as separate evidence.

07 Law, practice and your own choice

Commercial discussions often mix three types of statement: what the law permits, what people actually do, and the risk a company consciously chooses to accept. Confusing these creates false certainty. A widespread practice does not become lawful simply because others do it. Equally, a company must not present its own voluntarily stricter policy as a legal prohibition.

Case study: email address visible in a LinkedIn contact field

A decision-maker places an email address in the contact details of their LinkedIn profile. You know their name, organisation and role. Can you now send an unsolicited personal commercial email? Article 11.7(3) of the Dutch Telecommunications Act provides a B2B exception for electronic contact details which the end user has expressly designated and published for receiving such unsolicited communications, provided the intended use matches that purpose. [C37]

The strict interpretation: a general contact field is meant to make someone reachable by their network, not necessarily to receive unsolicited advertising. Publication alone does not demonstrate that specific designation. The broader interpretation: a person has consciously made their business address visible to their professional network and could in some circumstances reasonably expect a business approach. Neither interpretation is adopted here as a universal legal answer; the exact context, visibility setting and stated purpose require assessment.

An address such as firstname@company.nl does not, by itself, establish that Article 11.7(3) applies. With a private email address, the case for designation for business advertising is even harder to make. The sender must also separately assess the GDPR lawful basis and information obligations. [C37][C38]

One relevant personal email: a risk choice, not a right

In practice, an entrepreneur may decide to approach a single carefully selected person with relevant information. From a relationship perspective, that is very different from a thousand automated messages, but lower volume creates no statutory exemption. Where consent or an applicable channel exception is absent, this is a consciously accepted legal risk, not a practice endorsed by this whitepaper. [C37]

A request for contact through a genuinely non-commercial channel, a conversation following an invitation, or visible knowledge-sharing may offer another route. The distinction depends on purpose, implementation, personal data and platform rules. The practical approach is therefore to record the source and intent first and allow the route to commercial contact to emerge explicitly.

No myths about enforcement

'The regulator only looks at large campaigns anyway' is not a verifiable exemption. Without a specific, current primary source on enforcement, this whitepaper draws no conclusions about the priorities of ACM or the Dutch Data Protection Authority. The legal boundary and the likelihood of enforcement are two different questions.

Enforcement case by case: what the AP actually says

The enforcement policy adopted by the Dutch Data Protection Authority on 30 October 2026 offers no exemption for small personal campaigns. Where an infringement is ongoing, the AP seeks its termination; it chooses an appropriate instrument taking into account factors such as gravity, duration, intent, number of people affected, damage, cooperation and past conduct. A finding does not automatically lead to a fine, but a lighter intervention is not guaranteed either. [V01]

Under certain conditions, the AP can issue a warning before processing begins, issue a reprimand or corrective order, restrict or prohibit processing, or impose an administrative fine. An entrepreneur who stops voluntarily may have that taken into account as a circumstance, but doing so does not retrospectively legalise the original processing. [V01]

This policy concerns the AP and the legislation it supervises. It must not be used to predict separate ACM enforcement of unsolicited commercial communications. It contains no general policy of tolerating 'one personal email'. [V01][V02]

08 Tracking, pixels, retargeting and lookalikes

Access to the device: assess ePrivacy and the Dutch Telecommunications Act first

Article 11.7a of the Dutch Telecommunications Act and Article 5(3) of the ePrivacy Directive establish the general rule that storing information on, or gaining access to information in, a user's terminal equipment requires clear information and consent. Narrow exceptions exist for technically necessary communication and strictly necessary services; Dutch law also provides a limited exemption for information about quality or effectiveness where privacy implications are absent or minor. [B02][B04]

In Planet49, the Court confirmed that consent must be active: a pre-ticked box is not sufficient. Information must include, among other matters, the duration of cookies and third-party access. [B13]

A pixel also creates responsibilities

Fashion ID shows why 'it is the platform's pixel' is too simplistic. A website operator which integrated a social plug-in that automatically collected and transmitted visitor data could be a joint controller with the platform for collection and transmission. The Court limited that responsibility to operations for which the website operator actually participated in determining purposes and means. [B14]

The EDPB applies that reasoning to advertising targeting. An advertiser and a social media platform can be joint controllers for selecting audiences, matching and displaying advertisements. Where cookies or similar tracking are involved, Article 5(3) of the ePrivacy Directive must also be considered. A commercial interest can be legitimate but is not automatically sufficient for invasive profiling and cross-site tracking. [B15]

Custom audiences and lookalikes

In list-based targeting, the advertiser uploads identifiers such as email addresses or telephone numbers, which the platform matches against its own users. The EDPB treats the advertiser as a controller for the initial collection and as a joint controller for various subsequent targeting operations. The source, lawful basis, transparency, right to object and allocation of responsibilities must therefore be in order before the upload. [B08][B15]

NOT ALL ADVERTISING IS THE SAME

Advertising based on sector, context or a broad audience is legally different from retargeting an individual visitor or using a custom audience from your CRM. In a campaign builder, distinguish at least: contextual, platform audience, own list, website retargeting and lookalike.

09 Enrichment, scraping and LinkedIn data

Being public is not a lawful basis

The Dutch Data Protection Authority describes scraping as the automated collection and recording of information from webpages. Where personal data is involved, the GDPR applies in principle. The AP stresses that scraping for sales or marketing may be possible, but scale, sensitivity, reasonable expectations and the chosen lawful basis can make compliance difficult. [B16]

A public profile does not make its information 'free for use'. For indirectly obtained personal data, Article 14 GDPR requires information about purposes, lawful basis, categories, recipients, retention period and source, including whether the source was publicly accessible. That information must generally be supplied within one month and, where the data is used for communication, no later than the first communication. [B08]

Legitimate interests following KNLTB

Following the KNLTB judgment, it is too strict to say that a purely commercial interest can never be legitimate. The Court says that a commercial interest can constitute a legitimate interest, but necessity and the balancing test must still be satisfied. A smaller data model, clear recording of sources and evidence of the individual's reasonable expectations make the assessment more defensible; mass enrichment of unknown people makes it more difficult. [B06]

LinkedIn is not a legal free zone

A LinkedIn connection may provide context for reasonable expectations and for whether follow-up is appropriate, but it replaces neither channel consent nor the information obligation. The platform's terms of use and technical rules remain a separate layer alongside privacy legislation. This whitepaper therefore makes no general claim that 'every connection may be emailed'.

The same design principle applies to private messages and InMail: do not treat the platform as a back door. If the message is commercial, campaign-driven and directed at an individual, record source, relationship, purpose, objection route and platform rules. Whether a specific platform feature falls under the Dutch Telecommunications Act may depend on its technical and legal implementation and requires separate assessment before large-scale use.

Intent-signal tools and LinkedIn: is this permitted?

What has changed. A tool no longer reports only that 'this company is interested'; it may suggest that a particular decision-maker has purchasing intent. Sometimes this takes place through browser extensions or linked employee LinkedIn accounts. That means the source and processing require scrutiny. [C47]

Four overlapping layers. GDPR: individual signals may constitute personal data and profiling; assess the lawful basis, Article 14 and whether a DPIA is required by the level of risk. ePrivacy: identifying website visitors through cookies or fingerprinting may require prior consent. LinkedIn: unauthorised scraping and account automation may breach section 8.2 of the User Agreement. Dutch Cybersecurity Act (Cbw)/NIS2: assess the SaaS tool and its access to CRM, website and employee accounts under applicable supply-chain security obligations. Where AI is involved, also assess Articles 4 and 50 of the AI Act. [C47][C48]

Three cases. Proxycurl: LinkedIn brought proceedings against this provider of LinkedIn data in January 2025; according to reporting, the company ceased operations and was required to delete data obtained from LinkedIn. Apollo.io and Seamless.ai: industry publications reported that their LinkedIn company pages disappeared in March 2025; the cause was not officially established. Bisnode (Poland): collecting information from public registers did not remove the obligation to inform individuals under GDPR Article 14; the highest administrative court confirmed the key point while returning aspects of the fine and former entrepreneurs for further consideration. [C49][C50]

Ten questions for your supplier. 1. Is LinkedIn access officially authorised? 2. Does the tool automate connections, messages or scraping? 3. What are its sources, data categories and retention periods? 4. How is Article 14 complied with? 5. How are objections and deletion handled? 6. Which subprocessors and AI models are used? 7. What DPIA supporting information is available? 8. How do website identification and consent work? 9. How are security and incident reporting organised? 10. What role does the tool have under the AI Act? [C51]

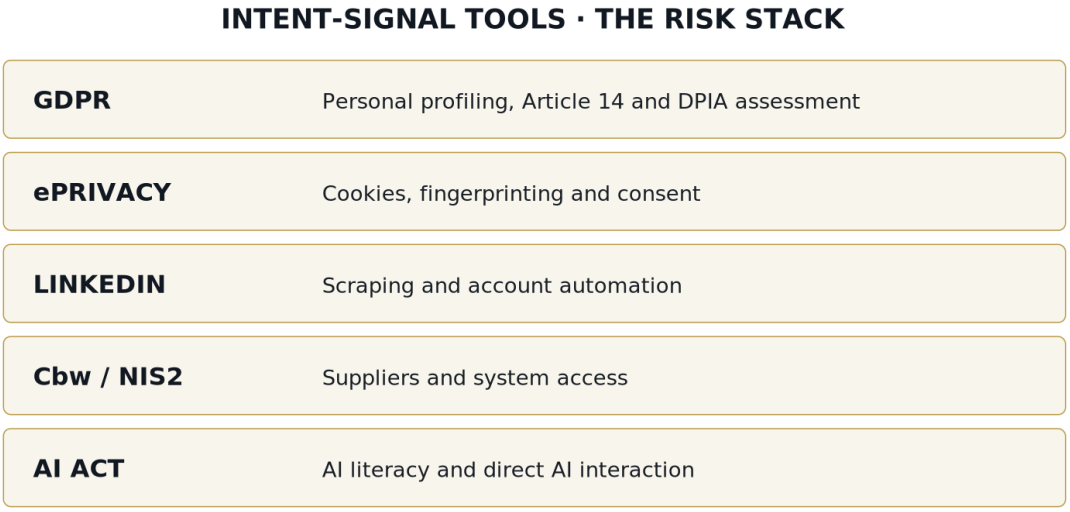


Figure 4. Layers of assessment for intent-signal tools. [C47][C48]

HCI design choice: organisation before individual

Organisation-level signals are legally attractive only while they cannot in fact be traced back to a natural person. Once visits, role, behaviour or profile attributes can directly or indirectly be linked to an identifiable individual, they become personal data subject to the GDPR. 'Organisation first, person later' is therefore not merely a marketing philosophy but also a data-minimisation choice. [B07]

10 AI agents in sales and marketing

Direct interaction: disclose that it is AI

The current AI Act requires providers of systems intended to interact directly with natural persons to design those systems so that people are informed they are interacting with AI, unless this is obvious in the particular context. An autonomous sales bot that handles email replies or SMS conversations may therefore be treated differently from an AI assistant that merely drafts a message for a person to check and send. [B18]

AI literacy: not just for developers

Article 4 of the AI Act already applies and was amended in 2026. Providers and deployers must take measures to support the development of AI literacy among staff and others operating systems on their behalf, taking account of knowledge, experience, education, context and the people on whom the systems are used. The current text expressly states that no specific level need be guaranteed for each individual. [B19][B21]

Profiling does not automatically trigger Article 22

A lead score or profile does not automatically fall under Article 22 GDPR. That provision covers decisions based solely on automated processing, including profiling, which produce legal effects or similarly significantly affect a person. Much sales prioritisation will not meet that threshold, but the underlying processing must still satisfy all other GDPR requirements. [B10]

The agent chain: controller, processor, subprocessor

Anyone using an external AI model or agent platform to process personal data must also arrange Article 28 GDPR compliance. A controller may use only processors providing sufficient guarantees; processing must be governed by a contract, and engaging subprocessors requires the agreed authorisation and flow-down of obligations. A Data Processing Agreement (DPA) matters, but a DPA does not itself create a lawful basis for the original submission of data. [B11]

Human oversight is not a universal fix

Human-in-the-loop processes are valuable for quality and risk management, but they do not legalise unlawfully collected data, prohibited tracking or a prohibited communication channel. The sequence remains: make the data and channel lawful first, then organise AI governance. That is why a sales agent cannot be designed independently of campaign, consent and source evidence.

DESIGN REQUIREMENT FOR AGENT STUDIO

A sales or marketing agent should know at least: its purpose, audience, channel, permitted data sources, evidence of relationship or consent, opt-out status, processor route, human escalation and the wording with which it identifies itself as AI when required.

Agent Studio: one shared source of legislation

Within HCI Agent Studio, legislation-focused agents work from one shared legislation collection. For each law, it contains a source reference and a verification date (geverifieerd_op). This provides traceability, not a guarantee that every legal outcome is correct or that an agent may independently issue legal judgments. [C39]

11 EU versus US: the same words, a different system

The mistake is not to claim that the United States 'has no rules'. The issue is that its rules are structured differently. A playbook configured lawfully in the US may still be unlawful in Europe because of the opt-in and device-consent model.

Topic	EU / Netherlands	United States (federal baseline / California example)
Commercial email	Prior consent is the general rule for unsolicited electronic marketing, subject to limited exceptions under Article 11.7 of the Dutch Telecommunications Act and ePrivacy. [B01][B03]	At federal level, CAN-SPAM mainly sets content, identification and opt-out obligations; the FTC does not state a general advance opt-in requirement for commercial email. Opt-outs must be honoured within 10 business days. [B24]
Cookies / retargeting	Storage of or access to terminal equipment generally requires prior consent. Tracking also triggers GDPR requirements. [B02][B04][B13][B15]	There is no single federal equivalent of the EU cookie-consent model. In California, businesses subject to CCPA must respect rights to opt out of sale or sharing, including cross-context behavioural advertising. [B26]
Automated SMS / calls	SMS is an electronic message and consent is the general rule. [B01]	The TCPA restricts robocalls and robotexts. Prior express written consent applies to certain regulated automated, artificial-voice or prerecorded telemarketing routes. The FCC one-to-one consent amendment was overturned by the Eleventh Circuit in 2025 and removed from the rules. [B25]
AI in commercial communication	AI Act transparency may apply to direct AI interaction. GDPR and ePrivacy continue to apply. [B18]	The FTC enforces existing rules against unfair or deceptive practices even when AI is used; there is no general AI exemption. [B27]
Maximum privacy / AI fines	GDPR: for the most serious categories, up to €20 million or 4% of worldwide annual turnover, whichever is higher. AI Act: up to €35 million or 7% for prohibited practices; other obligations in Article 99 have different maxima. [B12][B20]	CAN-SPAM: the FTC currently states up to $53,088 for each non-compliant email, alongside other possible consequences. TCPA has a distinct enforcement and civil-liability framework. [B24][B25]

Statutory maximum fines do not predict the penalty in any particular case. Regulators and courts consider the facts, seriousness, duration, culpability and other statutory factors. A maximum amount must therefore never be presented to a board as the 'likely fine'. [B12][B20]

EU / NL AND US · DIFFERENT RULES

EU / NETHERLANDS	US · FEDERAL
Email: opt-in as a general rule	Email: opt-out as a general rule
Tracking: consent to access devices	Tracking: federal/state patchwork
AI Act + GDPR + Dutch law	FTC + CAN-SPAM + TCPA + states

Figure 5. Simplified EU/US comparison, not comprehensive legal advice. [B01][B24][B25]

12 When are you being too strict?

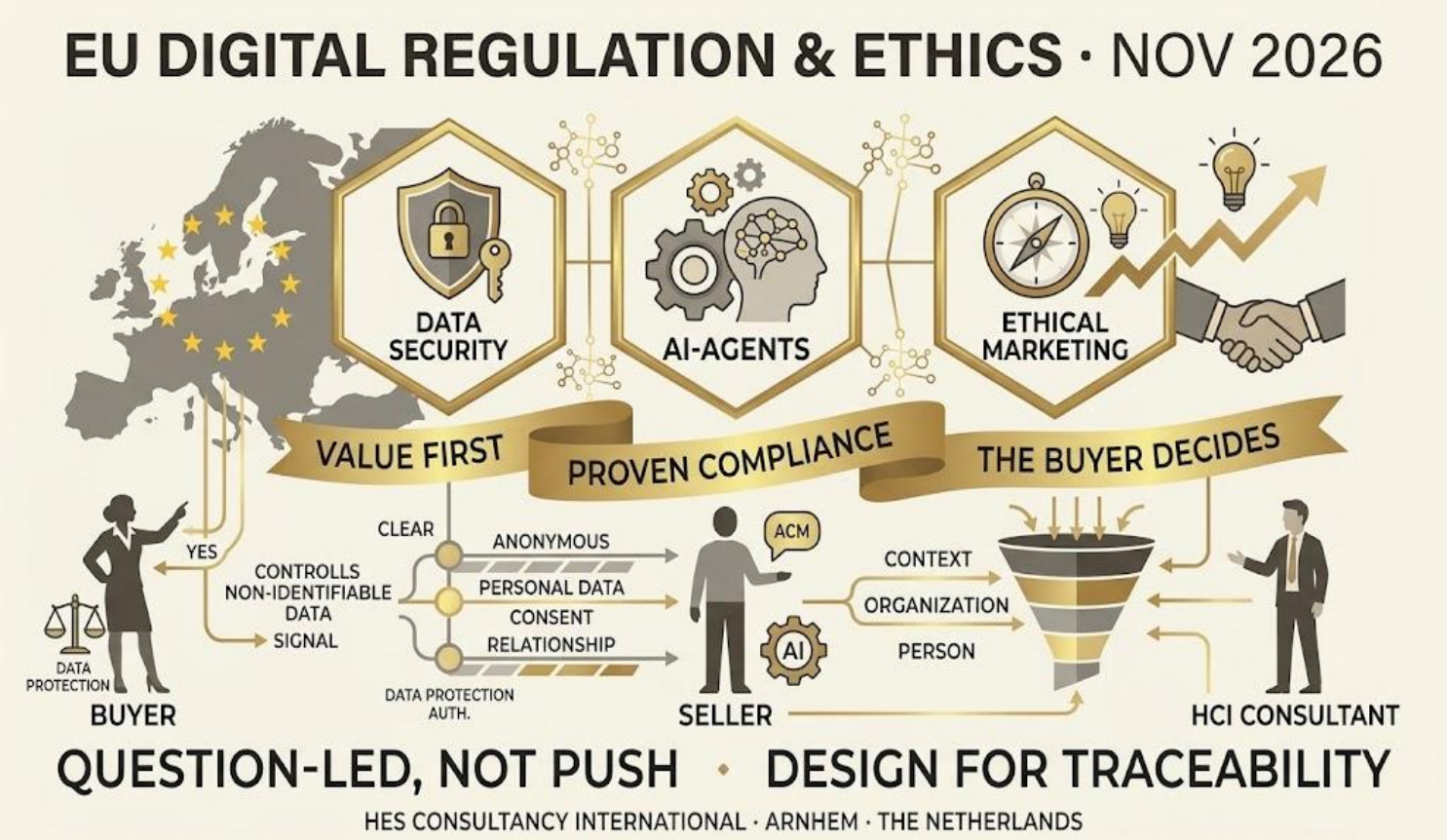
Compliance becomes counterproductive when every commercial activity is treated as prohibited as a precaution. The law does leave genuine room for action. That room must simply be linked to the correct legal provision.

Situation	Possible in principle	Condition / limitation
Responding to a specific inbound enquiry	YES	The communication was requested or is needed to supply the requested service. Do not silently reuse the details for another marketing purpose.
B2B email to an address expressly published for that purpose	YES, potentially	Only within Article 11.7(3): the contact details must have been designated and published for receiving such unsolicited communications. [B01]
Emailing an existing customer about a similar service	YES, subject to conditions	Contact details obtained in connection with a sale; own similar products or services; option to object at collection and in each message. [B01][B28]
Processing personal data on the basis of legitimate interests	YES, potentially	Record the interest, necessity, less intrusive alternatives, expectations and balancing test. [B06]
Stopping direct marketing after an objection	REQUIRED	Objection is absolute for processing for direct marketing. [B09]
Using organisation-level signals	YES, if genuinely non-personal	As soon as data can be traced to a natural person, the GDPR applies.
Privacy-friendly effectiveness measurement without individual tracking	YES, sometimes without cookie consent	Only within the narrow Article 11.7a(3) exception: quality/effectiveness measurement with no or minor privacy implications. [B02]
Using AI to edit an email written by a person	YES	AI Act transparency for direct bot interaction differs from internal use. Personal data, processing agreements and data minimisation still require attention. [B11][B18]

NOT MORE CATHOLIC — BUT ABLE TO PROVE IT

The better compliance question is not “is sales allowed to do anything?” It is “which route do we use, what evidence supports it, and where does the consent or expectation end?”

13 The HCI model: outside-in as a data architecture



HCI deliberately chooses a model in which the buyer is prioritised over the personal profile wherever possible. In some situations, that choice is stricter than the minimum the law might require. That is perfectly acceptable: an organisation may adopt a higher design standard, provided it does not present that choice as a statutory obligation.

Phase	HCI behaviour	Legal design check
1. Orientation	Whitepaper, page or scan landing page; do not identify visitors by default.	No marketing pixels before a valid choice. Keep functional/strictly necessary technology separate from tracking. [B02][B04]
2. Organisational signal	Aggregate interest at organisational level wherever possible.	Check that small groups or other characteristics do not allow identification of an individual.
3. Scan / report	Individual voluntarily supplies details to receive a report.	Record purposes and information duties. Make commercial follow-up separately visible or substantiate a specific exception. [B07][B08][B01][B05]
4. Relationship	Only relevant follow-up, with a centralised unsubscribe status.	A relationship informs expectations and balancing but does not replace channel consent. [B06][B09]
5. Strong signal	Multiple organisational signals prompt a human discussion with the vendor.	No automatic transfer of personal data without a lawful basis, transparency and role allocation.

Phase	HCI behaviour	Legal design check
6. Vendor action	Vendor and HCI agree who takes each step.	Identify controller/processor/joint controller roles and record the source of consent or relationship before transfer. [B11][B15]
7. AI assistant / agent	AI supports processes that are already lawful.	Article 50 transparency for direct AI interaction; AI literacy; human escalation. [B18][B19]

The key correction to “consent during the scan”

A scan form can provide a useful point of transition from anonymous visitor to known contact. However, 'leaving details to receive a PDF' and 'consenting to commercial nurturing' are not automatically the same legal event. The product design must separate those purposes. This does not weaken the model; it makes the outside-in promise visible and demonstrable. [B07]

What HCI deliberately does not need to do

- Build a personal profile before there is a concrete need and lawful basis.
- Allow a lead score to decide that someone “may” be emailed; channel rules remain separate.
- Upload a CRM list to an advertising platform without separate source and lawful-basis checks.
- Allow an AI agent to start autonomous follow-up using a vague opt-in combining report delivery, tracking and marketing.

14 Practical channel checklist

Channel	Green — how to design it	Red — do not do without an additional basis
Email	Answer inbound enquiries; use valid opt-in or a demonstrated Article 11.7 exception; identify the sender; provide simple opt-out. [B01][B28]	“They are on LinkedIn, therefore I may email them”; purchased list; unsolicited commercial email asking for consent.
LinkedIn / InMail	Be human and relevant; document relationship and purpose; follow platform terms; respect objections.	Use the platform as a legal bypass for mass individualised commercial outreach.
Website / scan	Function first; purpose for each field; privacy information; separate marketing choice; minimal retention. [B07][B08]	Automatically equate a report request with unlimited marketing consent.
Pixels / retargeting	Activate only after a valid choice where required; explain purposes and third parties; document roles. [B02][B13][B14][B15]	Fire a pixel in advance because the data is pseudonymised or held by the platform.
Custom audience	Assess source, lawful basis, expectations, objections, platform roles and transfers. [B15]	Upload CRM data merely because addresses were originally collected lawfully.
Scraping / enrichment	Keep it limited and purpose-bound; record sources; provide Article 14 information and an LIA where relevant. [B06][B08][B16]	Mass-copy public profiles and assume cold outreach is then permitted.
AI agent	Run only after data and channel gates; disclose AI identity where Article 50 applies; record processor chain and escalation. [B11][B18]	Let the agent decide consent “probably exists” or that silence constitutes consent.
US campaign	Configure CAN-SPAM, TCPA and state laws separately, with explicit geographic and recipient routing. [B24][B25][B26]	Reuse US settings unchanged for the EU/Netherlands.

Minimum evidence record for each identified individual

- source of the contact details;
- date and context in which they were obtained;
- purpose or purposes for which the details are used;
- GDPR lawful basis and, where relevant, the legitimate interest assessment reference;
- channel basis: consent, Article 11.7 exception or inbound/transactional context;
- wording and version of the consent statement where consent is relied upon;
- unsubscribe/objection status and date;
- any transfer to a vendor or platform and allocation of responsibilities;
- AI agent identifier and transparency/escalation rule where AI communicates directly.

A system unable to show these evidence records will also struggle in practice to demonstrate why a contact action was lawful and appropriate. This connects to HCI's wider message in The Perfect Storm: demonstrable accountability matters more than a policy document that merely says everything is in order. [B30]

15 What has changed since The Perfect Storm?

The reference date for this whitepaper is 1 November 2026. Several dates in earlier HCI publications have since been overtaken by legislation and must be updated before the material is reused.

Topic	Position as at 2 November 2026	Source
Dutch Cybersecurity Act (Cbw, NIS2) and Wwke	Both Dutch laws entered into force on 15 August 2026. For the Cbw the Dutch government describes registration, duty-of-care and notification obligations and board-level responsibility; the Wwke has separate designation, risk, duty-of-care and notification obligations.	[B22]
Cyber Resilience Act	Reporting obligations for actively exploited vulnerabilities and severe security incidents have applied since 11 September 2026. The Commission refers to 24 hours for early warning and 72 hours for full notification.	[B23]
AI Act — general application	The Regulation has generally applied since 2 August 2026. Following Regulation (EU) 2026/1744, high-risk obligations under Chapter III, Sections 1–3 apply from 2 December 2027 for Annex III and 2 August 2028 for Annex I.	[B21]
AI literacy	Article 4 has applied since 2 February 2025. Its amended 2026 wording requires measures supporting the development of AI literacy and states that a specific individual level need not be guaranteed.	[B19][B21]
Telemarketing in the Netherlands	Since 1 July 2026, unsolicited telemarketing to natural persons, including sole traders, generally requires prior consent. Existing customers do not have a general exemption. Calls to legal persons are not subject to the same natural-person rule. The email soft opt-in for existing customers is governed separately. [C40]	[B01]

DORA: relevant to the supply chain, not the general outreach rule

DORA (Regulation (EU) 2022/2554) has applied to the financial sector since 17 January 2025. It sets requirements for ICT risk management and ICT third-party arrangements, including contractual provisions and the register of ICT services. DORA does not directly determine whether an individual sales email may be sent. For a vendor serving financial institutions, the operational supply chain may nevertheless be assessed under DORA. [C41]

16 The small business without a database

A start-up often has no customer database, no established relationships and no list of valid marketing consents. The old formula is tempting: gather and enrich addresses, have a series of messages written, and use pixels to see who responds. But that very combination may trigger privacy, communications and platform rules at the same time. Limited resources do not reduce the legal thresholds facing a small entrepreneur.

The alternative route starts with content and with the buyer's situation. Publish knowledge about a concrete problem, explain organisational developments without unnecessarily tracking individuals, and offer a scan or assessment that someone may start voluntarily. The user chooses whether to answer questions, receive a report and separately consent to subsequent commercial contact. The buyer sets the pace.

Nxt Era: the platform approach

Nxt Era is free for user organisations. Suppliers and partners may have up to 5 active signals at the same time free of charge; a paid option for additional signals will follow later, only after prior notice and agreement. [C53]

Nxt Era is an invitation-based platform described by HCI for organisations seeking to connect supply and demand through signals they post themselves. Its user presentation distinguishes suppliers, partners and user organisations. Participation starts by signing up through an invitation; users provide their name, business email address and sector, and accept the terms and privacy statement. According to the presentation, other permissions are off by default. This describes the intended user experience, not an independently verified live audit. [V06]

The core is not a hidden lead score but mutual choice. A participant posts a signal (for example 'I am looking for' or 'I offer'), selects one to five topics, and sets the sector and duration. The presentation lists four signal types: Actively searching, Open, I offer and Follow only. Only the first three can result in proposals; the last cannot. A proposal arises only where demand and supply are compatible, a topic is shared, sector settings match and both signals are active. Simply visiting, browsing or clicking does not count as a buying signal. [V06]

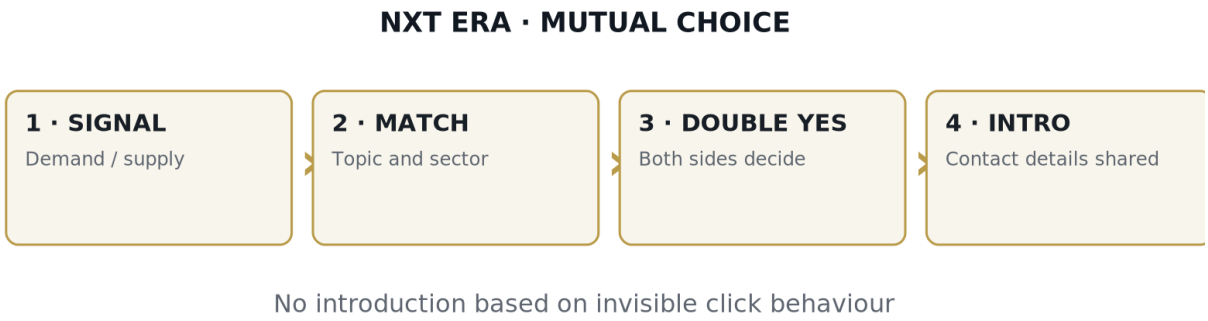


Figure 6. Nxt Era introduction process as described in the product terms. [V06][C52]

What a small business owner can do tomorrow

- Choose one sector-specific problem in which you can demonstrate expertise.
- Publish useful, freely accessible explanations without hidden individual-level tracking.
- Offer a scan or conversation and separate report delivery from marketing consent.
- Start with genuinely organisation-level signals and assess whether individuals can be identified.
- Record only contact actions for which the channel basis and origin can be demonstrated.

This guarantees no rapid growth. It does, however, make the route to a first customer less dependent on a purchased database and on the illusion that automation equals consent.

Calling businesses: what is permitted is not necessarily profitable

The Dutch telemarketing amendment of 1 July 2026 protects natural persons, including consumers, self-employed sole traders and partners in general partnerships, even when they act professionally. This specific opt-in rule does not apply in the same way to business calls to legal persons. Whether the number and subscriber genuinely fall within the corporate route requires checking; a director's private mobile number is not automatically a 'company number'. A lawful telephone call must also comply with other relevant rules, including the GDPR where personal data is processed. [V02]

What does calling achieve? Belkins analysed more than 175,000 dial attempts in 2025, mainly reflecting international sales-development practice. According to the supplier, 9.9% of attempts connected; 58% of those became conversations; 4.6% of conversations resulted in appointments. Together that represents approximately

0.26% of dial attempts, or one appointment per 370–380 attempts. The sample is not independent, representative Dutch research. [V03]

Scenario	Assumptions	Indicative effort / cost
Your own time	370 dial attempts; assumption: 60–80 attempts per day	Approximately 5–6 working days, excluding preparation, research and aftercare
Outsourced	Assumption: 60–80 dial attempts per eight-hour day; indicative agency rate of €50–€120 per hour	Approximately €1,850–€5,920 per appointment; illustration, not a quotation
Higher conversion	Some Dutch agencies cite 20–100 calls per appointment	Not comparable without the same audience, methodology and definition of an appointment

The calculation is deliberately transparent: 370 ÷ 80 to 370 ÷ 60 ≈ 4.6–6.2 calling days; at 8 hours a day and €50–€120 per hour, approximately €1,850–€5,920. Because these sources are not directly transferable, it cannot be concluded that calling is unviable for every start-up. Test conversion rates in your own segment before ruling out the channel. [V03][V04][V05]

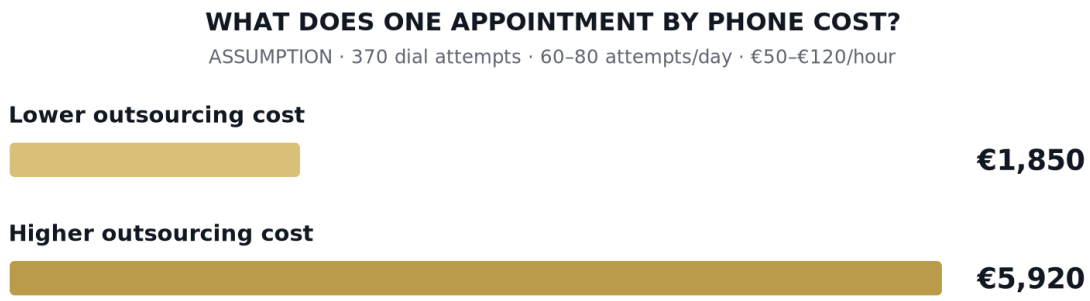


Figure 7. Illustrative scenario, not a measured Dutch cost per appointment. [V03][V05]

Five ways to obtain a warm introduction

A warm introduction is not the same as unlimited marketing consent. Obtain the intended contact's agreement to the specific introduction first. Record which party asked, and exactly what the 'yes' covered; do not automatically use the response for newsletters or extensive follow-up campaigns. [V07]

Route	Sequence	Legal and practical boundary
1. Personal network	Ask a relevant connection whether they know the prospect; that person first checks whether an introduction would be welcome, then sends a group introduction.	A one-off introduction is not an opt-in to future commercial mailings.
2. Vendor / partner	The partner asks their customer to agree to a specific introduction to HCI, or organises a joint session.	The existing-customer email exception does not generally authorise a partner to promote someone else’s product.
3. Webinar / round-table	Choose one subject; the partner invites via its own lawful channel; attendees register themselves.	Event registration and consent to later marketing are separate purposes.
4. Satisfied	Ask a customer whether they know someone; have the customer approach	Do not collect the addresses of acquaintances

customer	that person first and introduce you if they agree.	to email them without a request.
5. Matching platform	Buyers and suppliers post their own signals; relevance generates a proposal; contact details are released only following mutual agreement.	Consent to an introduction is not automatically consent to every subsequent commercial activity.

Becoming visible without an existing address list

A small business can build access to potential buyers without first buying a database of individual contacts. Choose one sector-specific issue, publish a useful article or short interpretation, contribute to trade publications and professional communities, and allow visitors to initiate a scan, assessment or conversation voluntarily on your own website. Keep report delivery, follow-up concerning the request and optional marketing consent separate; asking for information is not general newsletter consent. [V07]

For LinkedIn, the assertion that 'a personal profile works better' is a practice-based hypothesis here, not established Dutch effectiveness research. In practical terms, you can make a relevant connection without a pitch, comment substantively on professional topics, publish a sector-specific analysis and then link to public material on your own website. Reading or following a profile does not in itself constitute consent to personal email follow-up. [V07]

Step	Action	What is recorded
1	Define one specific problem for each ideal customer profile (ICP).	Problem, target audience and source supporting the claim
2	Publish open knowledge on your own website, LinkedIn or an industry channel.	Publication date, sources and owner
3	Offer a voluntary scan or substantive session.	Request, purpose and necessary contact details
4	Separate report delivery from optional marketing in the form.	Exact wording, channel, timestamp and affirmative choice
5	Use only suitable follow-up expressly wanted by the individual.	Evidence of request, introduction or valid channel basis

Nxt Era: how a proposal and introduction work

According to the supplied 26-step presentation, participants choose for each signal whether matching applies only within their sector or across sectors. There must always be a shared topic; cross-sector matches are possible only when both parties select that option. Before mutual acceptance, the other party normally sees only the role and job title; the organisation is shown only if the participant enables this for that signal. Names and email addresses are exchanged only when both sides say 'yes'. [V06]

There are two contact routes. (A) Based on two matching active signals, the system suggests a proposal; both parties decide independently. (B) Someone sees a relevant signal in Discover and requests an introduction; the recipient decides. If either side declines, the presentation says both parties see only that it did not proceed, without an explanation. Following mutual acceptance, the contact appears in Relationships. The presentation also describes a weekly email digest, the option to pause proposals, and signals that expire or can be extended after 14–90 days. [V06]

According to the supplied privacy statement (v1.0, effective from 14 October 2026) and Nxt Era terms, additional permissions are off by default and choices are logged. The product presentation describes data downloads, account deletion and hosting in Germany. The live operation has not been independently technically audited in this documentary review. [C52]

Nxt Era is no licence to use consent given for one purpose for another purpose. The principle is explicit mutual interest, with personal details released only after a double 'yes', never on the basis of invisible behaviour. This can give a start-up access to genuine demand without a purchased email list as its foundation. According to the product terms supplied by HCI, these principles appear in Nxt Era's privacy statement and terms: no AI processing of participant data, only necessary cookies, no links to other systems, hosting in Germany, and free use for user organisations. [C52][C53]

https://hes-consultancy-international.com/nxt-era

17 Conclusion: not less selling, but better design

'Are you more Catholic than the Pope?' is ultimately not a call to test the limits. It is a call to understand where the limits actually lie. The third question may be the hardest: does the entrepreneur even understand what an AI agent can access through their email, diary or files — and how can they find customers responsibly without a database?

Being too strict means treating every commercial interest as prohibited, assuming that all processing of personal data requires consent, or thinking an organisation may act only after a prospect explicitly requests a sales conversation. The GDPR provides other lawful bases. The Dutch Telecommunications Act contains exceptions. Inbound enquiries, existing customer relationships, business contact details published for a specific purpose and non-personal organisational signals provide genuine room for action. [B01][B06]

Being too permissive means copying an American funnel and assuming a lead magnet automatically authorises all follow-up; assuming a platform pixel lies outside your responsibility; treating a LinkedIn connection as email consent; or allowing an AI agent to infer legal permission from probability. [B01][B13][B14][B15][B18]

The sustainable approach lies between those extremes. Give buyers value first. Collect personal data only when there is a concrete reason. Make purposes visible. Retain evidence. Keep channel rules separate from GDPR lawful bases. Allow AI agents to act only within boundaries already established by people and technology. And always give the buyer an easy way to withdraw.

THE HCI POSITION IN ONE SENTENCE

Outside-in means not only that the customer sets the pace. It means you can demonstrate that pace in your data model, consent flow and agents.

Have your actual campaigns, consent wording, vendor roles, platform configurations and cross-border data flows reviewed by an ICT/privacy lawyer before going live. This document is not legal advice.

Sources and legal references

The legal sources were consulted on 1 and 2 November 2026, including ACM material, AP enforcement policy and the Belkins methodology. Reference codes [Bxx], [Cxx] and [Vxx] are used throughout. Internal HCI sources describe the product rather than establish legal validity.

C42 Microsoft, Work Trend Index, “Breaking down the infinite workday”, 17 June 2025: average of 117 emails and 153 Teams messages; interruption statistics relate to the busiest 20% of users and exclude EU tenants.
https://www.microsoft.com/en-us/worklab/work-trend-index/breaking-down-infinite-workday

C43 Gartner, “Sales Survey Finds 61% …”, 25 June 2025, and “67% …”, 9 March 2026. Different surveys (632 versus 646 buyers), not a panel tracking the same respondents.
https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-sales-survey-finds-61-percent-of-b2b-buyers-prefer-a-rep-free-buying-experience ; https://www.gartner.com/en/newsroom/press-releases/2026-03-09-gartner-sales-survey-finds-67-percent-of-b2b-buyers-prefer-a-rep-free-experience

C44 Gartner, survey of 645 B2B buyers, May 2026: 69% want to validate AI-generated insights with a sales representative.
https://www.gartner.com/en/newsroom/press-releases/2026-05-20-gartner-survey-finds-sixty-nine-percent-of-b-two-b-buyers-turn-to-sales-reps-to-validate-ai-generated-insights

C45 Mike Hes, personal observations in conversations from 2021 to 2026; PAC RADAR and Whitelane Research are referenced as market sources, not quantitative evidence supporting those observations.

C46 Dutch Data Protection Authority (Autoriteit Persoonsgegevens), Datalekkenrapportage 2024 (2024 Data Breach Report), published July 2025, p. 22: incidents arising when personal data was entered into AI chatbots.
https://www.autoriteitpersoonsgegevens.nl/system/files?file=2025-07%2FRapportage+datalekken+2024.pdf

C47 GDPR Articles 4(4), 5, 6, 14 and 35; ePrivacy Directive Article 5(3); Dutch Telecommunications Act Article 11.7a. Assess profiling and high-risk processing case by case.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

C48 LinkedIn User Agreement, section 8.2; Dutch Cybersecurity Act, depending on the type of entity concerned; AI Act Articles 4 and 50.
https://www.linkedin.com/legal/user-agreement

C49 LinkedIn / Proxycurl and Apollo.io / Seamless.ai: secondary industry reporting; the cause and exact scope of proceedings have not been independently verified from primary sources.
https://www.socialmediatoday.com/news/linkedin-wins-legal-case-data-scrapers-proxycurl/756101/ ; https://martech.org/a-pair-of-lead-gen-providers-have-disappeared-from-linkedin/

C50 UODO, 20 September 2023, Bisnode ruling (III OSK 2538/21): failure to fulfil information duties; fine and part of the scope remitted for reconsideration.
https://www.uodo.gov.pl/en/553/1572

C51 Mike Hes, Risk Assessment: Signal-Based GTM Tooling, 8 October 2026, section 8, ten due-diligence questions; internal assessment checklist, not an independent legal source.

C52 Nxt Era, privacyverklaring v1.0 (privacy statement), effective since 14 October 2026; publicly accessible source URL not independently readable at the time of review.
https://pilot.nxterasolutions.eu/privacy

C53 Voorwaarden Nxt Era v1.1 (Nxt Era terms and conditions, November 2026); conditions supplied by HCI, not yet published at the time of review.
https://pilot.nxterasolutions.eu/voorwaarden

B01 Netherlands — Dutch Telecommunications Act (Telecommunicatiewet), Article 11.7; statutory basis Stb. 2021, 103, as amended by the Energiewet (Energy Act), Article 7.8 (Stb. 2025, 12), effective 1 July 2026 (Stb. 2025, 89).
https://zoek.officielebekendmakingen.nl/stb-2021-103.html ; https://zoek.officielebekendmakingen.nl/stb-2025-12.html ; https://zoek.officielebekendmakingen.nl/stb-2025-89.html

B02 Netherlands — Dutch Telecommunications Act (Telecommunicatiewet), Article 11.7a (storing/accessing information on terminal equipment; exceptions).
https://wetten.overheid.nl/BWBR0009950

B03 Directive 2002/58/EC (ePrivacy Directive), Article 13 — unsolicited communications.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

B04 Directive 2002/58/EC (ePrivacy Directive), Article 5(3) — storage/access to terminal equipment.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058

B05 Court of Justice of the European Union, 13 November 2025, C-654/23, Inteligo Media, ECLI:EU:C:2025:871, particularly operative part 1–2 and paragraphs 40–69.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CJ0654

B06 GDPR Article 6(1)(f), recital 47; Court of Justice of the European Union, 4 October 2024, C-621/22, KNLTB, on legitimate commercial interests, necessity and balancing.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/ ; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0621

B07 GDPR Articles 4(1), 4(11) and 7 — personal data and definition/requirements for consent.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

B08 GDPR Articles 13 and 14 — information when data is collected directly or indirectly; source information.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

B09 GDPR Article 21(2)–(4) — objection to direct marketing.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

B10 GDPR Article 22 — solely automated decisions producing legal or similarly significant effects.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

B11 GDPR Article 28 — processors and subprocessors.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

B12 GDPR Article 83(5) — maximum administrative fines for serious infringements: €20 million or 4% of worldwide annual turnover, whichever is higher.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

B13 Court of Justice of the European Union, 1 October 2019, C-673/17, Planet49, ECLI:EU:C:2019:801 — active cookie consent, duration and third parties.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0673

B14 Court of Justice of the European Union, 29 July 2019, C-40/17, Fashion ID, ECLI:EU:C:2019:629, paragraphs 81–85 — joint controllership limited to processing operations jointly determined.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CJ0040

B15 EDPB Guidelines 8/2020 on the targeting of social media users, version 2.0/2.1, including paragraphs 43–46, 50–56, 61–65, 71–72 and 93–96.
https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

B16 Autoriteit Persoonsgegevens, Handreiking scraping door particulieren en private organisaties (Guidance on scraping by individuals and private organisations), April 2025.
https://www.autoriteitpersoonsgegevens.nl/system/files?file=2025-04%2FHandreiking+scraping_april+2025.pdf

B17 Autoriteit Persoonsgegevens, Reclame/direct marketing (Advertising/direct marketing) — lawful basis, consent and information obligations.
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/direct-marketing

B18 AI Act, Regulation (EU) 2024/1689, consolidated text of 27 July 2026, Article 50(1).
https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng

B19 AI Act, consolidated text of 27 July 2026, Article 4 as amended — AI literacy.
https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng

B20 AI Act, consolidated text, Article 99 — maximum administrative fines.
https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng

B21 AI Act Article 113 and Regulation (EU) 2026/1744 — amended application dates for high-risk AI.
https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng ; https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32026R1744

B22 Rijksoverheid (Government of the Netherlands), 15 August 2026 — entry into force of the Dutch Cybersecurity Act (Cbw) and Critical Entities Resilience Act (Wwke); principal obligations.
https://www.rijksoverheid.nl/actueel/nieuws/2026/08/15/cyberbeveiligingswet-en-wet-weerbaarheid-kritieke-entiteiten-vanaf-vandaag-van-kracht

B23 European Commission, Cyber Resilience Act — reporting obligations effective from 11 September 2026; 24-hour/72-hour deadlines.
https://digital-strategy.ec.europa.eu/en/policies/cra-reporting

B24 FTC, CAN-SPAM Act: A Compliance Guide for Business — requirements, opt-out, 10 business days and current penalty amount.
https://www.ftc.gov/business-guidance/resources/can-spam-act-compliance-guide-business

B25 FCC TCPA rules, Eleventh Circuit Insurance Marketing Coalition v FCC, No. 24-10277 (24 January 2025), and FCC conforming final rule 2025.
https://docs.fcc.gov/public/attachments/FCC-24-24A1.pdf ; https://media.ca11.uscourts.gov/opinions/pub/files/202410277.pdf ; https://federalregister.gov/d/2025-16641

B26 California Attorney General, CCPA — right to opt out of sale or sharing; “sharing” includes cross-context behavioural advertising.
https://www.oag.ca.gov/privacy/ccpa

B27 FTC, Operation AI Comply, 25 September 2024 — existing consumer protection rules also apply when AI is involved.
https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

B28 ACM, Spam voorkomen in uw reclame (Preventing spam in advertising) — consent, existing-customer exception and opt-out; ACM as regulator.
https://www.acm.nl/nl/verkoop-aan-consumenten/reclame-en-verleiden/spam-voorkomen-uw-reclame

B29 Aletto, Five Steps to Book 100+ Demos, 14 May 2026 — American sales playbook used solely as a practical example; its marketing figures are not treated as independent facts.
HCI-provided reference material

B30 HCI, De Perfect Storm (The Perfect Storm), April 2026 — tone and earlier compliance context; obsolete statutory dates have not been reused unchanged.
HCI-provided reference material

B31 HCI vision and strategy, recorded 31 October 2026 — outside-in approach, buyer control, signals and internal standards of conduct.
HCI-provided reference material

C33 GDPR Articles 2(2)(c), 5(1)(b) and 6(4): household exemption and purpose limitation.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

C34 GDPR Article 28 and Chapter V: processors, contracts and possible third-country transfers. Product settings require separate assessment.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

C35 GDPR Article 14: information obligations and exceptions where data is obtained indirectly.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

C36 AI Act Article 4, consolidated version of 27 July 2026 (amended by Regulation (EU) 2026/1744): measures to support AI literacy.
https://eur-lex.europa.eu/eli/reg/2024/1689/2026-07-27/eng

C37 Dutch Telecommunications Act (Telecommunicatiewet), Article 11.7(1), (3), (4), applicable from 1 July 2026: the purpose for which published business contact details were designated and the exceptions.
https://wetten.overheid.nl/BWBR0009950

C38 GDPR Articles 6, 13, 14 and 21: lawful basis, information and the right to object in direct marketing.
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng/

C39 HCI Agent Studio: one legislation collection holding a source reference and verification date (geverifieerd_op) for each law. Internal product architecture, not an independent legal source.

C40 ACM, 2026 telemarketing changes effective 1 July 2026, and Dutch Telecommunications Act Article 11.7: natural persons, sole traders and existing customers; separate email soft opt-in.
https://www.acm.nl/nl/publicaties/vanaf-1-juli-strengere-regels-voor-telemarketing-alleen-nog-maar-als-klant-toestemming-heeft-gegeven ;
https://wetten.overheid.nl/BWBR0009950

C41 DORA, Regulation (EU) 2022/2554, Articles 2, 5–16, 28–30 and 64; applicable from 17 January 2025.
https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng/

V01 Autoriteit Persoonsgegevens, Handhavingsbeleid (Enforcement Policy) of 30 October 2026, sections 2.1–2.3, 3.1.1–3.1.7, 4.2, 5.2, pp. 3–19. Original source: AP Doc 2026.pdf.
https://autoriteitpersoonsgegevens.nl/actueel/handhavingsbeleid-ap-gepubliceerd

V02 Autoriteit Consument & Markt, “Vanaf 1 juli strengere regels voor telemarketing” (Stricter telemarketing rules from 1 July), published 25 June 2026, and Dutch Telecommunications Act Article 11.7.
https://www.acm.nl/nl/publicaties/vanaf-1-juli-strengere-regels-voor-telemarketing-alleen-nog-maar-als-klant-toestemming-heeft-gegeven

V03 Belkins, B2B cold calling statistics 2026: benchmark research based on over 175,000 dials from 2025. Supplier data, primarily from outside the Netherlands; not independent Dutch research.
https://belkins.io/blog/cold-calling-benchmarks

V04 Leadworks, “Hoeveel cold calls zijn nodig voor één afspraak?” (How many cold calls are needed for one appointment?); agency claim of 20–100 calls, not independently validated.
https://leadworks.nl/hoeveel-cold-calls-zijn-nodig-voor-een-afspraak/

V05 Telesales Direct, “Wat kost telemarketing uitbesteden?” (Cost of outsourced telemarketing): €50–€120 per hour; indicative commercial source, not nationwide price statistics.
https://www.telesalesdirect.nl/kennisbank/wat-kost-telemarketing-uitbesteden/

V06 HCI, “Nxt Era – How it works”, English version 6, 26 slides; HCI-supplied user presentation. Product operation described by the material, not independently tested live.

V07 HCI, “Hoe dan wel?” (How should it be done?), 2 November 2026. Five introduction routes, LinkedIn practice-based hypotheses, channels and assumptions; not a primary legal source.

HES CONSULTANCY INTERNATIONAL
YOUR BUSINESS MY SERVICES