

Marijam Özdemir / Tobias Theelen

6 DATA PRIVACY MISTAKES ALMOST EVERY COMPANY MAKES





INTRODUCTION

Does this sentence sound familiar?

☐ **"I have read and accept the privacy policy."**

This checkbox is often found beneath various online forms ... and it's completely superfluous. There is no need to accept a privacy policy because it merely serves an informational purpose.

Since the GDPR / UK GDPR was introduced, there has been some panic surrounding consent and the legal basis for data processing. Every company must have a privacy policy on its website but contacts do not have to "accept" the policy to justify data processing. Some other consents are required, but we'll discuss those later.

Our customers often face the same GDPR issues around data protection and information security. These mistakes can have vastly different consequences – ranging from slight inconveniences through to negative reviews on comparison sites or hefty fines. They include:



1. Incorrect email dispatches
2. CV databases of headhunters and HR departments
3. Incorrect and superfluous checkboxes beneath website forms
4. Lack of employee training on data protection topics
5. Incorrect assignment of responsibilities between processors and controllers
6. Fear of supervisory authorities

We will now look at each one of these mistakes and show you how to best avoid them.



CONTENT

Incorrect email dispatches	4
CV databases of headhunters and HR departments	7
Incorrect and superfluous checkboxes beneath website forms	10
Lack of employee training on data protection topics	13
Incorrect assignment of responsibilities between processors and controllers	16
Fear of supervisory authorities	19
Summary	21



INCORRECT EMAIL DISPATCHES

SOME BACKGROUND INFORMATION

It's one of the classic cases of data protection infringement: sending emails while cc'ing recipients who shouldn't be there in the first place. And you might be thinking, "That won't happen to me!" But unfortunately, our daily experiences prove otherwise. Having a visible list of recipients continues to be one of the most common data breaches in companies.

Each and every day, there are millions of emails sent with other people in the cc (carbon copy). Usually, nothing happens. The cc recipients can see the exact email addresses to which the message was sent – similar to the regular recipients. What's more, the entire email history is visible. This can lead to problems if there are recipients who...

- should not become aware of the email addresses of the other recipients;
- can access personal information that should not be shared with them from the email history.

THE LEGAL SITUATION

If an email address can be assigned to a natural person, it is considered to be a piece of personal data in accordance with Art. 4 (1) UK GDPR. And such information may only be provided to a third party with either consent or with another legal basis in place. If the email address is shared, as is the case with a visible email list, this constitutes a data protection infringement.

HERE'S A PRACTICAL EXAMPLE OF SUCH AN ERROR

An association wishes to inform all its members and a list of interested parties about a legal update. Therefore, the board of the association drafts a small newsletter and to directly distribute the newsletter to all recipients, the email addresses of members and interested parties are copied into the cc field. Of course, all recipients do receive the update, but they can also see all the email addresses of the other members. This is a clear breach against the protection of personal data from a privacy perspective.



Another example: A logistics company is looking to drive its Q1 revenues in 2021 and grants new customers who conclude a contract in Q1 a 20% discount. A sales employee wants to directly inform three companies that she's currently negotiating with. To save some time (and deadlines are always tight in sales), she decides to cut a corner and sends an email to one of the possible new customers, putting the other in cc. Now personal data has been disclosed and even worse, the recipients now know the other companies also in negotiations.

FINES

In 2018, the Independent Inquiry into Child Sexual Abuse (IICSA) was fined £200,000 after a member of staff sent a bulk email to participants in the inquiry. Unfortunately, the staff member added recipients' email addresses into the 'To' field rather than blind copying them. This meant that recipients of the email had access to other people's email addresses, some of which included first and last names. Given the sensitive nature of the cause, more should have been done to prevent this from occurring.



DOING IT RIGHT

There's a very easy solution to this data protection gaffe:

1. Don't use the cc field, use the bcc field below it. Bcc stands for "blind carbon copy" – recipients in this field can only see the sender of the email and the contents or history of the mail.
2. Take some time for another check before forwarding email histories. Is all the information in the email really suitable for the new recipients?
3. When sending newsletters, we recommend using dedicated tools that directly allow and store other data protection principles such as consent and the double opt-in process, whilst sending unsubscribe links too.
4. All this can only work properly in practice if employees are trained in the handling of personal data. But more on that in chapter four.

 To: checker23@p-online.com justine.h@jahoo.com catlover@hub.com
hercules88@coldmail.com estolo@creative.com mueller@it-consulting.co.uk
dustin.kleeberg@xtra.co.uk prof.dr.james.warren@email.com

CC:

BCC:

SUBJECT:
Important Notice: Changes to General Terms and Conditions!



CV DATABASES OF HEADHUNTERS AND HR DEPARTMENTS

SOME BACKGROUND INFORMATION

Wouldn't it be convenient to store all applicants' data indefinitely? This way, you'd have a bunch of suitable candidates for every vacancy, and all you need to do is contact them.

This is such a promising idea. Many HR departments and headhunters create entire databases of resumes and employer references – it sounds great, but it's not exactly legal.

THE LEGAL SITUATION

Resumes, employer references, and applicant files are classed as personal data. They can only be processed and stored if there is a legal basis (Art. 6 UK GDPR). If this legal basis no longer applies, the data must be deleted. What's more, data subjects (applicants) must, among other things, be informed of the purpose and duration of data processing, as described in Art. 13 UK GDPR.

Art. 6 UK GDPR lists the following legal basis for the processing of personal data:

- Consent of the data subject
- Necessary for the performance of a contract
- Necessary for compliance with a legal obligation
- Necessary to protect the vital interests of the data subject
- Necessary for the performance of a task carried out in the public interest
- Necessary for the purposes of the legitimate interests pursued by the controller



The Data Protection Act 2018 (DPA 2018) provides the legal basis for data processing during the application process while the Information Commissioner's Office (ICO) has also issued guidance on this in the form of the Employment Practices Code. As a best practice, only personal data that is relevant to the recruitment decision should be collected.

After rejecting an applicant, the application documents may be stored for a certain legally permissible period, but they must be destroyed/deleted after this period expires.

Data may only be stored beyond this period with the consent of the data subject. The duty to provide information in accordance with Art. 13 (UK GDPR) must always be observed. Data subjects must be informed of the data processing, among other things.

- Purposes of data processing
- The legitimate interests that underpin the legality of data processing, if these provide the legal basis for processing.
- Information on transmitting data outside the UK
- The duration of data processing
- Reference to the right to provide information, submit a complaint, and withdraw consent

FINES

No fines have yet been imposed for the storage of applicant data beyond the application process. One of the highest fines imposed so far, however, is based on a very similar situation that occurred in Germany. Property company Deutsche Wohnen stored data on tenants and rental applicants for many years without having an erasure policy in place. The fine: a whopping 14.5 million euro. The problem with storing applicant data? There is no legal basis in place – and this is what happened to Deutsche Wohnen.



DOING IT RIGHT

Companies have to scrutinise the process they have in place for applicants.

Were applicants already informed of the purpose and duration of data processing? If this is not the case, relevant information can be added to the email that is sent to confirm receipt. Is there an erasure policy in place for applicant data or request for consent to longer storage – for example, to be considered for future vacancies?

Many recruiters have long been using professional networks, such as Xing and LinkedIn, to stay in contact with applicants. This comes with benefits and drawbacks. On the one hand, applicants continuously update their LinkedIn profile and reaching out to them is easy. On the other hand, the connections made in this way are lost when a recruiter leaves the company.



INCORRECT AND/OR SUPERFLUOUS CHECKBOXES BENEATH WEBSITE FORMS

SOME BACKGROUND INFORMATION

Data processing for marketing purposes is very often underpinned by the legal basis of data subject consent. No surprise, with most other legal basis being irrelevant for contacts who are not yet customers. Companies are eager to go hunting for consent. But not every consent is useful – and the actually important information is sometimes left out when companies are busy creating checkboxes.

THE LEGAL SITUATION

The UK GDPR does not provide any boilerplate templates for checkbox designs – even if many companies would be happy to have them. What the UK GDPR does do, however, is provide clear guidelines on the process behind obtaining consent.

We recommend including at least the following elements on the form:

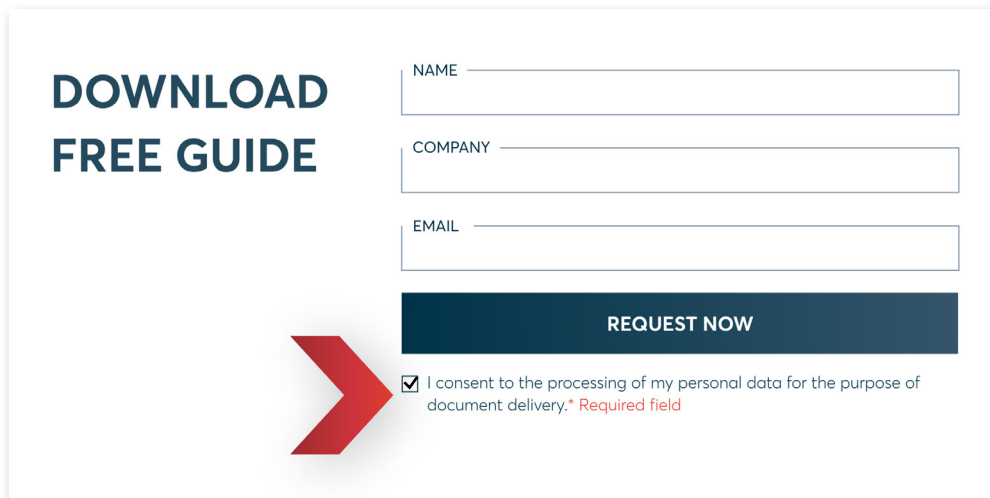
- Information on the purpose of data collection (principle of purpose limitation pursuant to Art. 5 (I) (b) UK GDPR)
- Reference to the option to withdraw consent
- **Voluntary** checkbox for a consent to the distribution of marketing information and/or sales reaching out to the consenting party

In accordance with Art. 7 UK GDPR, consent must be given freely to be effective. Art. 7 (4) UK GDPR says the following:



"When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

SOME WIDESPREAD ERRORS



The screenshot shows a form titled "DOWNLOAD FREE GUIDE". It contains three input fields: "NAME", "COMPANY", and "EMAIL". Below these fields is a dark blue button labeled "REQUEST NOW". To the left of the button is a large red arrow pointing right. Below the arrow is a checkbox that is checked, followed by the text: "I consent to the processing of my personal data for the purpose of document delivery.* Required field".

In this example, the customer is not being given the opportunity to give clear, unambiguous consent for their data to be used for marketing purposes. This is an example of bundled consent, where the consent request is bundled into the agreement of the acceptance of a privacy policy. The ICO guidance advises against this because it does not meet the UK GDPR criteria for valid consent, that is a freely given, specific, informed and an unambiguous decision.



DOING IT RIGHT

Just to recap: the UK GDPR makes no explicit statements on how to create checkboxes. This allows companies to adapt consent to the specific purpose of data collection and processing.

Make sure to: separate the necessary from the optional. If a website visitor requests to receive a checklist by email, there's no way around data processing for exactly this purpose. More detailed marketing information – such as a newsletter – is, however, optional. Make sure to never mix these two purposes – consent to a newsletter must stay voluntary.

Consent must be given by choice, and not a requirement to receive a freebie such as an e-book or webinar. Here's what this might look like:

DOWNLOAD FREE GUIDE

NAME

COMPANY

EMAIL

REQUEST NOW

☐ I consent to the processing of my personal data for the purpose of document delivery.* Required field

☐ I consent to the processing of my personal data for marketing purposes such as product and service announcements and newsletters.
You have the right to revoke your consent at any time.



LACK OF EMPLOYEE TRAINING ON DATA PROTECTION TOPICS

SOME BACKGROUND INFORMATION

You might have the strictest security measures for your server rooms, cleverest encryption, and most watertight Data Processing Agreement in place – no piece of data is safe if your employees become careless. Employee training is one of the key tasks of a data protection officer (DPO) under the UK GDPR.

THE LEGAL SITUATION

The UK GDPR defines the tasks of a DPO to include the following:



"[...] monitor compliance with the UK GDPR and other data protection laws, and with your data protection policies, including managing internal data protection activities; **raising awareness of data protection issues, training staff** and conducting internal audits"
[emphasis added by the editors]

However, the UK GDPR does not specify what such training should look like. Here too, the data protection officer has quite a bit of leeway. The law does not prescribe any given training form (online, in person, only written training, ...) or course refresher cycles either. Processing operations usually evolve continuously, new technologies are used, and people tend to forget what they've learned if they don't repeat it. That's why we at DataGuard recommend at least annual training intervals.

SOME EXAMPLES OF EMPLOYEE TRAINING TOPICS

Besides the data protection principles, employees should be instructed on the rights of data subjects. Other topics include company data protection guidelines, data protection when using mobile devices, as well as the legal basis and other specialist terms. It is particularly important to instruct employees on how to behave in the event of data breaches and data protection infringements. Employees who are in direct contact with customers, should additionally become aware of what information they may share with customers – and the conditions for sharing.

Try to make the training as interesting as possible and avoid merely ticking off topics with exhausting theory. Include examples of data protection in daily business and interactive elements to help keep employees focused during the training and raise awareness for the tasks they will later perform.

To make concepts such as Records of Processing Activities (ROPA), Technical and Organisational Measures (TOM), and other documentation obligations more tangible, it helps to run through practical exercises on specific data processing operations. Besides all this, training sessions should focus on aspects of data protection that are relevant to the specific daily activities of the employee. This helps illustrate the effects of certain processes. Those who are not only familiar with the theory of data protection, but also the practical side of things, can identify and steer clear of obstacles.

CONTENTS

- Data protection principles
- Legal basis
- Rights of the data subject
- Data protection guidelines of the company
- BYOD and the general use of mobile devices
- Conduct in direct contact with customers, partners, employees, applicants, and other external stakeholders
- Behaviour in the event of a data protection infringement

FORMAT

- Many practical examples
- Interactive
- Available online on demand, if possible
- Role-specific training, depending on the area of activity





FINES

A case in 2019 highlights the repercussions of not getting data protection right. A former company Director, David Cullen collected and illegally sold data to solicitors to enable the solicitors to identify potential clients. These potential clients had been involved in road traffic accidents, the solicitors wanted information so they could pursue personal injury claims on behalf of the potential new clients. Mr Cullen was not only fined, but also struck off as a Company Director for five years.



DOING IT RIGHT

This is where we would like to make some barefaced self-promotion. With the DataGuard Academy, DataGuard developed a platform that both trains employees on UK GDPR principles and offers role-specific training sessions, e.g. for IT experts and employees working from home.

[You can currently register for a free preview of the basic course!](#)



Generally speaking, internal data protection officers (DPO) often find it hard to motivate their team for training courses. This is easier for external service providers with learning platforms and interactive materials.



INCORRECT ASSIGNMENT OF RESPONSIBILITIES BETWEEN PROCESSORS AND CONTROLLERS

SOME BACKGROUND INFORMATION

Managing customer data in a SaaS CRM (such as Salesforce, Pipedrive, and HubSpot), having payroll accounting handled by a third-party provider, or simply sending a newsletter about marketing software – these are all examples of processing on behalf. The controller offers instructions to another company (the processor), which then processes data. Time and again, there are uncertainties about which party is responsible for which responsibilities. Should a CRM provider create a privacy policy for its customers?

THE LEGAL SITUATION

The interpretation of the definition of processing on behalf of a third party under the UK GDPR may be:



"[...] the collection or use of personal data by a processor in accordance with the instructions given by a controller and governed by a contract."

Here's the crux of the matter: all processing takes place on the basis of the controller instructions. This means that the controller is also responsible for the creation of a privacy policy, and the processor must be included in their Records of Processing Activities. The agreement that governs the collaboration is called a Data Processing Agreement and is usually created by the processor. The processor, on the other hand, must list the relevant processing activities in their "Records of Processing Activities" pursuant to Art. 30 (2) UK GDPR.



THE RIGHT WAY TO DO IT: UNDERSTANDING THE OBLIGATIONS OF THE CONTROLLER AND PROCESSOR.

THE OBLIGATIONS OF THE CONTROLLER

1. Making sure that the Data Processing Agreement really covers all requirements listed in Art. 28 UK GDPR. Particular care should be taken to ensure that:
 - a. there is a well-defined performance specification that precisely illustrates which partial performances are made by the processor
 - b. data categories are illustrated in detail; do not merely scratch the surface
 - c. there is a list of sub-processors of the processor in place, with evidence provided on the inspection of their data protection compliance
2. Check the Technical and Organisational Measures (TOM) of the processor. The TOM demonstrate how securely processors handle their customer data. These are an essential component of data processing agreements. The following aspects should be covered, for example:
 - a. Encryption measures
 - b. A breakdown of who has access to which data
 - c. Information on server redundancy and server security to guarantee availabilities
 - d. A reference to the multi-client capability of your solution
 - e. Comments on multi-factor authentication (e.g. for admins), if available
 - f. The purpose of the collected data, to demonstrate that only those data are collected that are necessary for the provision of the service
 - g. Information on patch management and regular updates
 - h. Notes on the remote maintenance process
3. Whenever relevant, the creation of a Data Protection Impact Assessment. The use of new technologies – such as SaaS solutions – in processing operations, can pose particular risks to the rights and freedoms of your customers and employees. These might require a Data Protection Impact Assessment.

THE OBLIGATIONS OF THE PROCESSOR

The processor is responsible for processing the data in line with the instructions of the controller. The principles of the UK GDPR that also apply to other companies must be observed.

This is joined by an important and often forgotten obligation: If an instruction of the controller infringes against the UK GDPR, the processor must inform the controller accordingly (Art. 28 (3)). There is an additional obligation to report data breaches to the controller (Art. 33 (2)).

In our [Whitepaper for SaaS providers](#), we explain how you can not only meet your relevant obligations but can also turn data protection into a competitive edge – for example by making sure that data protection concerns do not result in delays in the sales process.





FEAR OF SUPERVISORY AUTHORITIES

BACKGROUND INFORMATION

There are some letters nobody likes to receive... at all. And the tax authority, courts, banks, and supervisory authorities are no exception – no news is usually good news. However, there is no reason to get worked up when the ICO (the supervisory authority) gets in touch. Our advice: keep your cool. And above all: cooperate and never shy away from communicating with the ICO.

THE LEGAL SITUATION



The ICO acts in an advisory and guidance role as the UK's data protection watchdog. However, as part of this role they have several enforcement tools available implemented within the Data Protection Act 2018. The powers available to them include:

- Information Notices
- Assessment Notices
- Enforcement Notices
- Penalty Notices

Besides consulting, the ICO also has a supervisory role, making sure that rules are complied with. Cooperation with the ICO is one of the tasks of the data protection officer, pursuant to Art. 39 UK GDPR. If the ICO reaches out to you, the DPO should take it from there.

If a data protection breach has been identified in your company, you have to independently report it to the ICO within 72 hours. If the event comes with a high risk, you additionally have to inform the data subjects.



Risks to the personal rights and freedoms of data subjects	Notification obligation to the ICO?	Notification obligation to data subjects?
LOW	 Yes	 No
MEDIUM	 Yes	 No
HIGH	 Yes	 Yes

PRACTICAL TIPS FOR DEALING WITH THE ICO

In our role as an external DPO, we are in continuous contact with the ICO and we can usually lay all fears to rest. The ICO are communicative and cooperative and are quick to provide a friendly response to questions you might have. If the ICO requests certain documents, it is important that you act in a proactive and careful manner. An open cooperation with the ICO can certainly have a mitigating effect on later rulings.

With data breaches, it is crucial to meet all deadlines. Even if you might experience a 'deer in the headlights' response, or are eager to sweep the incident under the carpet, this is exactly what you should never do. Immediately report incidents to the ICO to demonstrate that your company takes data protection seriously, and this helps prevent higher fines in the end.

FINES

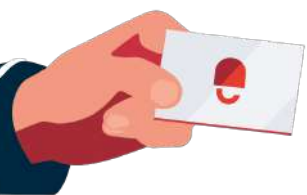
Credit reference agencies Experian, Equifax and Transunion were all investigated by the ICO for what they class as invisible processing. They were found to be ["trading, enriching and enhancing people's personal data without their knowledge."](#) Whilst Equifax and TransUnion made improvements suggested by the ICO, Equifax did not go far enough and were subject to an enforcement notice from the authority.



SUMMARY

With some hyperbole, our experiences show that no company manages to get everything right when it comes to data protection. There are quite a few pitfalls and obstacles that can lead to mistakes and misunderstandings. What's important is to stay on the ball, continuously scrutinise one's own data protection organisation, and make continuous improvements.

Your internal Data Protection Officer might be overwhelmed by the complexity of this topic, which is why we offer our "Privacy-as-a-Service" model with expert insights on demand – combined with our proprietary data protection platform with prioritised to-dos and continuously updated data privacy documentation.



DataGuard is a Compliance software company focused on Data Privacy and Information Security. As a European leader in the Compliance SaaS category, we enable over thousands of SMB and Corporate customers to automate and operationalise Privacy, InfoSec, and Compliance ("PIC") with ease. Our end-to-end SaaS solution drastically reduces the time and money companies spend to comply with privacy legislation such as GDPR, manage consents and preferences, and obtain infosec certifications such as ISO 27001. This enables our customers to focus on their core business, create value through trust and compliance, whilst mitigating risks and preventing breaches. We have offices globally in Munich, Berlin, London, and Vienna.



**Let's talk about your challenges
and define first steps on your
compliance journey:**

Contact us

You might also like:

- [Data privacy compliant cookie management and tracking](#)
- [On-Demand Webinar: GDPR Audit 101](#)
- [Overview of all data privacy documents from the UK GDPR](#)