LOYENS & LOEFF

DATA PROTECTION
& PRIVACY

Summer Dive 2020

LOYENS & LOEFF

So far in 2020, the Belgian Data Protection Authority has been quite active. In the period between January and September 2020, it has issued a total of ten administrative fines (ranging from EUR 1,000 to EUR 600,000) and issued administrative decisions in more than fifty cases, about half of which were published on the DPA's public website. The large majority of these cases were initiated upon complaint of an individual (against a former employer, a government body, an ex-partner, etc.). Three cases were initiated following an own-initiative inspection by the DPA.

The Loyens & Loeff Data Protection & Privacy Team has prepared updates throughout summer to help you keep up with these decisions. Our tips & tricks have been summarized per topic. Don't hesitate to reach out if you would like to receive more detailed guidance on any of these topics.

Have a nice read!

Content

1. Cookies

In its decision no. 12/2019, the BDPA issued recommendations on the compliant use of cookies and similar technologies. Below, we have included a basic cookies checklist:

- Know exactly **which cookies** (and similar technologies) you place and use reliable tools for cookie mapping (inadequate mapping can be qualified as negligence)

- Cookies information to be available in all **languages** of the website or application, intelligible taking into account the target audience, actively brought to the users' attention, and easily accessible from the home page of a website

- Consent required for **all non-functional cookies**, including analytical and statistical cookies

- **Informed consent** means that certain essential information must be included in the cookies banner itself (e.g. identity of data controller, categories of cookies, their purposes and which data they collect, right to withdraw consent, etc.)

- **Consent must be active, prior to placing cookies** (i.e. empty box the user must actively tick, use of sliders, etc.) - not acceptable: pre-ticked box, consent “by further browsing”

- **Consent must be free**, i.e. no cookie walls, no consent in exchange for a 'benefit' or 'reward'

- **Consent must be specific**, i.e. per type/category of cookie in first layer (second layer preferably includes cookie-per-cookie consent option)

- Consent by a user should be able to be **proven** at any later stage

- Add required GDPR wording (cf. article 12-13 GDPR) if the use of cookies entails a **processing of personal data** (e.g. IP address)

- **Lifespan/retention** of the cookies should be transparently disclosed and limited according to their purpose (e.g. keeping the shopping basket until the order is placed)

- Disclose which **third parties** have **access** to cookies

- Right to easily withdraw **consent (and preferably in a granular manner)** should be made explicit

- Instructions (preferably per Internet browser) on how the user can **delete** the cookies placed on his/her device (by for example referring to the possibility to delete cookies via specific browser settings)

- Verify how **changes** to the cookies policy will be (actively) brought to the user’s attention (e-mail, pop-up when visiting site or application, etc.)

Reach out to us if you wish to receive more detailed guidance on the applicable cookies legislation and regulatory guidance in the Benelux or Switzerland.

2. Designation and tasks of your Data Protection Officer

The entering into force of the GDPR on 25 May 2018 may have resulted in an obligation for your company to appoint a data protection officer ("DPO"). Through several decisions, the Belgian Data Protection Authority ("DPA") has in the meanwhile issued guidance on the designation of a DPO, and on the position/function of a DPO within your company.

Designation of a DPO

- The DPO must above all have excellent knowledge of data protection legislation.

- Extensive knowledge of internal IT systems and of business processes is of course valuable. Knowledge of data protection legislation is, however, a requirement for exercising this function and not a mere "plus".

- It is crucial to verify whether the DPO you have appointed or want to appoint fulfils such quality requirements, also if it is an external DPO - Request evidence of the fulfilment of quality requirements and document this evidence (e.g. successful completion of a "certified DPO" training, ISO certification, prior experience, IAPP CIPP/E of CIPM certificate).

Position and tasks of the DPO

- The DPO must be able to independently exercise his/her function within the company and conflicts of interests must be avoided.

  According to the DPA, there is a conflict of interest if the DPO is also head of compliance, risk management and internal audit (no independent supervision possible - as head of these departments, the DPO determines the purposes and means of the personal data processing of these departments).

- The DPO must be informed and, most importantly, consulted in advance on all matters relating to data protection. Merely informing the DPO of a decision after the decision has been taken renders his/her function ineffective.

- Reporting to the top management body cannot be limited to an annual report.

- It is not up to the DPO to actually decide on requests made by data subjects. Such decisions should be taken by the data controller.

As the DPA recently imposed several fines for not respecting the legal obligations regarding the designation and position/function of a DPO, it is highly recommended to verify whether your DPO fulfils the basic requirements set out above.

We are of course happy to assist if you have doubts in this respect.

3. Processing of photographs and (surveillance) video's

In several decisions in cases initiated upon complaints of data subjects, the Litigation Chamber of the Belgian Data Protection Authority ("DPA") has shed some light on GDPR compliance when processing photographs and/or video's. The majority of the decisions relates to the (un)lawful use of video surveillance camera's (CCTV), which are also governed by the Belgian Camera Act of 2007 (as updated to ensure alignment with the GDPR).

Below, we have summarised the main takeaways in relation to this topic.

Processing of photographs

- Use of a Facebook profile picture requires **a proper legal basis** (art. 6 GDPR) to be available, even if the photograph is publicly accessible, without restrictions. GDPR also applies to publicly available information.

- Information made publicly available on social media / Internet does not fall within "*purely personal or household activity*".

- **Balance of legitimate interests** (art. 6.1.f GDPR) can be an appropriate legal basis under the GDPR (but *quid* image rights legislation?) for the processing of photographs. Data minimization can be achieved by cropping the photo and removing image of persons other than the data subject who needs to be identified.

- Balance of legitimate interests less likely to be achieved when photo's of children are involved.

Processing of video's / CCTV

- DPA reiterated the importance of correctly **designating the data controller** for the operation of any CCTV system (e.g. the Association of Co-Owners in case of CCTV for an entire apartment building).

- **Balance of legitimate interests** (art. 6.1.f GDPR) can be an appropriate legal basis for CCTV, if balance is in practice indeed respected. Consent is often less appropriate (e.g. not valid if acceptance of CCTV is mandatory element of apartment purchase agreement).

- CCTV implemented in full **compliance with Camera Act of 2007** (notification to the police, use of mandatory pictogram, 30 days retention period, internal record, etc.) does not preclude the DPA from establishing an infringement of the GDPR (both types of legislation must be simultaneously applied and cumulatively complied with).

- Internal data processing record (art. 30 GDPR) may include section/tab with **specific CCTV processing record** (as required by the Camera Act of 2007), or alternatively, two separate records can be kept.

As the processing of personal data included in photographs and camera images has been identified as a key social issue and enforcement priority in the DPA's Strategic Plan for 2020-2025, this topic certainly warrants prioritisation in any compliance programme.

Reach out to us if you wish to receive more detailed guidance.

4. Fines imposed on digital services providers

In two recent decisions, the Litigation Chamber of the Belgian Data Protection Authority ("**DPA**") has imposed administrative fines on digital services providers. A fine of EUR 50,000 was imposed on a social network operator, and a fine of EUR 600,000 (highest administrative fine so far) was imposed on Google Belgium.

These decisions are however not only relevant for digital services providers. The most important "lessons learned" are summarized below.

Social network operator

- Belgian DPA volunteered to be the '**lead authority**' in this case. Given the cross-border nature of the data processing activities, 23 EU supervisory authorities had declared their involvement.

- Case referred to Inspection Service of Belgian DPA by Management Committee. Report of Inspection Service was transferred to Litigation Chamber, which found the **"invite-a-friend" practices** of the social network operator to be non-compliant.

- Social network users had to import their address book, which meant that contact details of ‘non users’ ended up on the social network's servers. When adding contacts, members of the network were confronted with pre-ticked options, whereby their contacts were already selected.

- Litigation Chamber found that:
  - defendant had no legal ground for storing and processing the personal data of non-users of and using them to send an invitation e-mail;
  - **only the data subject whose personal data are processed can validly consent** to the processing of his/her data, except in cases of parental consent or another legal power of attorney;
  - a user of a social media platform cannot give valid consent in the name and on behalf of a non-user of the social media platform; and
  - the storage of contact information of non-users can only be necessary in the context of "compare and forget" processes, and under certain strict requirements and safeguards.

- The social network operator also invoked the “**household exception**” included in article 2, §2, c) GDPR. However, the DPA confirmed that the GDPR does apply to controllers or processors providing the means for processing personal data for such personal or household activities. They themselves cannot benefit from the “household exception”.

Google Belgium

- Activities of Google Belgium and Google LLC were deemed to be inextricably linked, and the **Belgian subsidiary/establishment of the US data controller** can therefore be held liable.

- Fine imposed for failure to comply with the **right to be forgotten**, after Google rejected the data subject’s request to remove from its search results outdated articles that damaged his reputation.

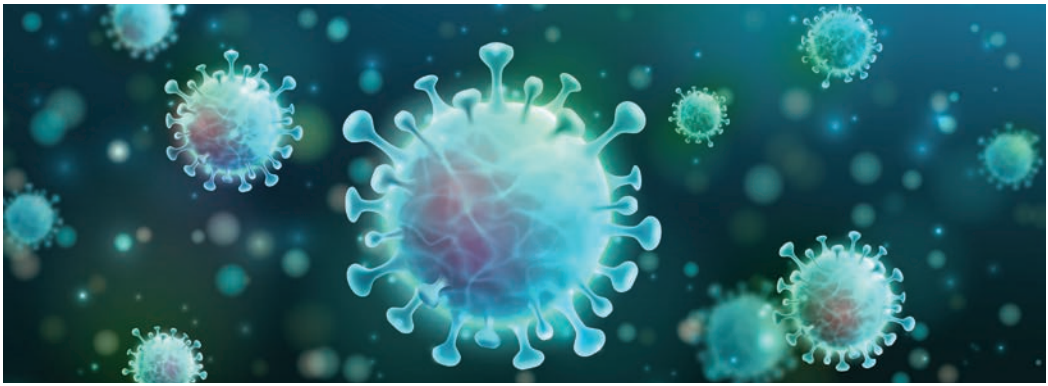
- Litigation Chamber considered that a **fair balance must be struck** between the public's right of access to information, on the one hand, and the rights of the person concerned, on the other hand.

- Regarding web pages referring to possible links with a political party, the Litigation Chamber found in Google's favour. It took the view that, considering the plaintiff's role in public life, maintaining these pages in the search results was necessary for public interest reasons. Regarding the pages referring to a complaint against the plaintiff, it ruled that the request for removal was well-founded and that Google was negligent in refusing the request because it had evidence that the facts were irrelevant and outdated.

- Also the lack of proper communication of the exact **reasons for the refusal** of the deletion request by Google, and the lack of **transparency** in the Google application form for deletion requests were emphasized.

- Order to de-reference imposed by Belgian DPA extends to Google search results made available in the **entire European Economic Area**.

Want to know more on how these decisions might impact your business? Don't hesitate to reach out!



5. Data Protection @ Work (Part 1/2)

In these difficult times, finding the right balance between protecting employee health, on the one hand, and data protection on the other hand, is not always easy. Below, we have analyzed a couple of questions with which employers often struggle these days. Our answers are based, among other things, on the official position of the Belgian Data Protection Authority.

Is it possible to impose COVID-19 tests on employees before being allowed back to work?

- An employer **cannot impose a COVID-19 test** on his employees purely based on the employer's authority. After all, this affects the physical integrity of the employees.

- The **processing of health data** is prohibited under Article 9.1 of the GDPR unless an exception is made by law or if the person concerned gives specific, free, informed and explicit consent. In the relationship between employee and employer, the employee's consent is rarely "free", given the hierarchical context and the fact that an employee may be under great pressure to consent.

- In the absence of a specific legal basis, an employee can therefore not be forced to undergo a test. It is, however, important to emphasize that staff members could be obliged to have themselves tested based on **other legal requirements**, for example when they are employed in the medical sector or when returning from holidays abroad.

Is it possible to take temperature tests before letting employees enter the employer's premises?

- The employer, through his hierarchical line and/or any other person (social worker, independent nurse, security guard, etc.), is **not allowed to run temperature tests** on his employees, or to require any certificate of good health before allowing an employee to enter the workplace, just as the employer may not involuntarily impose temporary incapacity for work or sick leave on his employees.

- Measuring body temperature is considered as collecting information about the state of health of a body, which is therefore considered to be a **medical act**, especially if the ability to work is linked to it. Such action is the prerogative of the treating physician or the occupational physician who can then refer to the employee's treating physician.

- In case of doubt about clinical symptoms in the workplace (coughing, headache, rhinitis, fever, muscle pain, etc.), the employer can refer the employee to his treating doctor or, if necessary, to the occupational physician who can give medical advice.

Is it possible to let employees fill in a questionnaire regarding COVID-19 symptoms?

- An organization can **never oblige employees to complete a questionnaire** regarding COVID-19 symptoms as this is considered a processing of health data.

- Like testing, the processing of health data is prohibited under Article 9.1 of the GDPR unless under the conditions described above. Given that there are currently no specific exceptions made by law, the free consent of the employee is required, but very difficult to validly obtain.

Which requirements must be fulfilled by employees after returning from vacation?

- Testing requirements have been implemented by the Belgian government regarding travels to COVID-19 affected areas. These rules apply between citizens and the public authorities, but of course they have immediate impact on the employment relationship.

- If an employee decides to **travel to COVID-19 affected areas**, this employee will have to bear the consequences imposed by the government. The obligations differ depending on the "code" of the area.
  - ***Green area***: There is no problem, the employee returns to the workplace or continues to work as before.
  - ***Red area***: The employee is required by law to go into quarantine (please note there are certain exceptions to this obligatory quarantine). The employee is also required to undergo testing (imposed by the government). The employee will have a certificate to stay home.
    An employer may refuse workplace access on the basis of this information. However, the employer will not always be aware of the travel destination (see below).
  - ***Orange area***: The government recommends the employee to be quarantined and tested but does not impose this after a stay in the orange area (as opposed to the red area). An employer can therefore not refuse access to the workplace if an employee returns from an orange area, as long as it is not established that the employee is incapacitated for work by a medical certificate from a physician. In other words, the employer cannot oblige the employee to go into quarantine. If the employer refuses entry,

the employer will have to pay the full remuneration to the employee if he cannot work from home. If the employer refuses to do so, there is a risk that the employee will claim compensation.

- The only possibility in this case is to instruct/ask these employees not to come to work after their return from an orange area, but to go to the personal physician first.

- Please note that the color given to a holiday destination should be checked at the moment the employee returns. The color code given to the area at the time the employee starts his vacation is not relevant. The color codes of the countries are updated daily on the website of the Federal Government: https://diplomatie.belgium.be/en.

Is it possible to let the employees fill in a questionnaire regarding their travel destination?

- Employees cannot be obliged to communicate where they are travelling in their private time, nor can an employer forbid his employees to travel to a risk area.

- Of course, an employer can voluntarily inquire about the holiday destination of employees who are planning to go abroad. Completion of a questionnaire is only possible if the employee can freely refuse to complete the questionnaire without being adversely affected (see above).

Reach out to us if you wish to receive more detailed guidance. We can of course also assist with the drafting of corporate policies for dealing with COVID-19 when employees return to work after their annual leave.

6. Data Protection @ Work (Part 2/2)

In some of its recent enforcement decisions, the Belgian Data Protection Authority ("**DPA**") has given further guidance on the application of the GDPR in an employment/HR context.

Below, we have summarized our key findings in this respect, noting that the DPA has also expressly stated that it is not its intention to interfere with the competences of the labour courts, only to enforce compliance with the GDPR.

GDPR in the recruitment process

Accepted as legal ground for retaining job candidates' personal data (of course taking into account purpose limitation and storage duration): explicit opt-in consent at occasion of job interview (e.g. by having candidates sign a consent form) + clear and unambiguous opt-out possibility for inclusion in recruitment database.

Exchange of information between former and current employer

- Purely oral disclosures or oral transfers of information between a former and current employer do not fall within the scope of the GDPR if none of this information is processed automatically or included in a file.

- The legitimate interests of an employer can cover the processing of personal data for its defense in (threatened) legal proceedings against a former employee. The legitimate interest must however be real and present, and the data processing must be necessary and proportionate for the legal defense purpose.

'Sensitive' employee data

Article 10 GDPR concerns data relating to criminal convictions or offences. This type of personal data is deemed to be particularly sensitive and therefore deservers additional legal protection (i.e. a general prohibition of processing such data, with only very limited exceptions). This protection does however not extend to any type of non-criminal 'judicial data' (as was the case pre-GDPR in the Belgian Privacy Act of 1992).)

Data subject rights in HR context

- When requested, access should be given to underlying documents substantiating the decision not to re-appoint someone for a certain mandate of function (= "essential information"), of course taking into account the rights and freedoms of others (e.g. colleague who reported an incident or made a confidential complaint) and the protection of trade secrets and other confidential information of the company.

- The right to data deletion is not an absolute right, data does not have to be deleted if processing is based on the presence of a legitimate interest which outweighs the data subject's interest to have certain data deleted.

- A data deletion request can be refused if the personal data concerned is not (or no longer) included in a computer system, database or file.

Processing of personal data by employees

The employer is deemed to be the responsible "data controller" for all personal data processing activities carried out by its employees during the execution of a task entrusted to them by their employer. In this capacity, employees act on behalf of their employer cannot separately and individually be qualified as "data controllers".

We remain of course happy to provide further guidance on any of the topics discussed above.

7. Data Subject Rights

In several recent decisions, the Litigation Chamber of the Belgian Data Protection Authority ("**DPA**") provided guidance on how to deal with data subject rights under the GDPR.

The most important "lessons learned" are summarized below.

General remarks

- Reply to data subject request must be unambiguous and clear. Exact **reasons for the refusal** to comply with a data subject request should be clearly and transparently communicated.

- Also a refusal / impossibility to comply with a request must be communicated within **1 month** after receiving the request.

- **Proof of identity** cannot be systematically requested from every person submitting a data subject request. It can only be asked if there are reasonable doubts about the identity of the person making the request.

- **Technical incapacity** to comply with well-founded data subject request is not a proper justification for not complying with the request.

- Data subjects do not need to expressly label their requests under the GDPR. The data controller needs to assess whether a request is **sufficiently clear** to be identified as a GDPR data subject request.

- Whenever **multiple (independent) data controllers** process the same personal data following consent given to one of them, the data controller that received a data subject request must take all appropriate measures to also inform the other date controllers hereof and to ensure that all of them comply with the request (and inform the data subject of any problems in this respect).

Right of access to personal data

- Data access requests can be denied if **short retention periods** cause the relevant data to no longer be available.

- When **replying in "different phases"** to broad/unspecified access request: at least the general information listed in articles 15.1(a)-(h) and 15.2 GDPR should be provided within 1 month.

- Article 15.3 GDPR does not require an original version or entire copy of the document containing personal data (e.g. an internal audit report) to be made available to the data subject. The right to **obtain a copy of his/her personal data**, does not imply that the data subject has the right to obtain a copy the full, original document containing these data, as this could infringe the rights and freedoms of others.

- The fact that the data subject would **already be aware** of the data of which a copy is requested, does not justify a refusal to comply with such a request.

Right to object

- A right to **object to direct marketing** messages (whether in electronic or paper format) is unconditional. It must be immediately complied with and the direct marketing data processing must immediately cease without any further investigation.

- The right to object to direct marketing messages **must be expressly, clearly and separately brought to the attention of data subjects** (in particular in each and every direct marketing message). It is not sufficient to only mention it in a privacy statement.

- Making an effective right to object **readily available** is an essential element of the "balancing of legitimate interests" test under article 6.1(f) GDPR.

Right to deletion of data ('right to be forgotten')

- Right to data deletion is **not an absolute right**, the data does not have to be deleted if processing is based on the presence of a legitimate interest.

- A **fair balance must be struck** between the public's right of access to information, on the one hand, and the rights of the person concerned, on the other hand.

Want to know more on best practices to comply with data subject rights? Don't hesitate to reach out!

8. Transparency & Privacy Policy - common mistakes

When drafting a privacy policy or privacy statement, there is one golden rule: describe what you *actually* do. Transparency is key!

Nevertheless, in practice, we see that this golden rule is often not fully respected. This has not escaped the attention of the Belgian Data Protection Authority, which has imposed various sanctions on companies for failure to comply with the transparency requirements.

Below you can find an overview of "common mistakes", together with some do's & don'ts.

No correspondence with reality

The privacy policy should always reflect the actual reality of the data processing operations. However, data processing operations included in the privacy policy are often incomplete or incorrect and do not fully correspond to reality.

- ***Don't***: use standardized templates or use the same privacy policy for all group entities without further review.
- ***Do***: map your data flows in your internal processing record and draft a tailormade privacy policy based on this mapping exercise.

Forgetting about 'further processing' of personal data or other changes in your data flows.

Data collected for one purpose may become interesting to process for a new purpose other than that for which the data were initially collected. The data subject must be informed thereof prior to such further processing.

- ***Don't***: consider having a privacy policy as something that you can cross of your 'to-do list' once and never have to look at again.
- ***Do***: regularly update your data flows in the internal processing record, adjust your privacy policy accordingly, and actively notify data subjects of such changes prior to implementing them.

Not informing data subjects whose data you have obtained from a third party

When you process personal data that you have not obtained directly from the data subject, but e.g. through a business partner, you should timely inform the data subject thereof (limited exceptions exist).

- ***Don't***: assume that the third party from whom you received the data has lawfully collected the data and/or informed the data subject of the disclosure of their personal data to you.
- ***Do***: actively review the privacy policy of this third party and verify whether you still have an information obligation, or fall under one of the exemptions of art. 14.5 GDPR.

Not specifying which legitimate interests you rely on

If you rely on legitimate interests for processing personal data, you must specify such legitimate interests in accordance with article 13.1.d) GDPR.

- ***Don't***: state, for example, in vague terms that the processing is based on your legitimate business interests.
- ***Do***: state, for example, that the processing is based on your legitimate interests as a company to promote your products or services towards existing clients for business development purposes.

Not mentioning how changes to the privacy policy will be communicated

- ***Don't***: merely state that the privacy policy may be subject to changes from time to time.
- ***Do***: include how you will bring changes to the privacy policy to the attention of data subjects (e.g. per e-mail or through a pop-up screen when visiting the website).

Do these common mistakes set alarm bells ringing? Want to have your privacy policy fully and thoroughly reviewed? Don't hesitate to reach out!

Contact

Stéphanie De Smedt
Attorney at law / Senior Associate
T +32 2 773 23 77
E stephanie.de.smedt@loyensloeff.com

Kim Lucassen
Attorney at law / Partner
T +31 20 578 52 39
E kim.lucassen@loyensloeff.com

LOYENS & LOEFF

LOYENSLOEFF.COM

As a leading firm, Loyens & Loeff is the logical choice as a legal and tax partner if you do business in or from the Netherlands, Belgium, Luxembourg or Switzerland, our home markets. You can count on personal advice from any of our 900 advisers based in one of our offices in the Benelux and Switzerland or in key financial centres around the world. Thanks to our full-service practice, specific sector experience and thorough understanding of the market, our advisers comprehend exactly what you need.

Amsterdam, Brussels, Hong Kong, London, Luxembourg, New York, Paris, Rotterdam, Singapore, Tokyo, Zurich

20-09-EN-SD