

Alexandra Jaspar
Director APD-GBA

Safeguarding data protection rights in Corona times

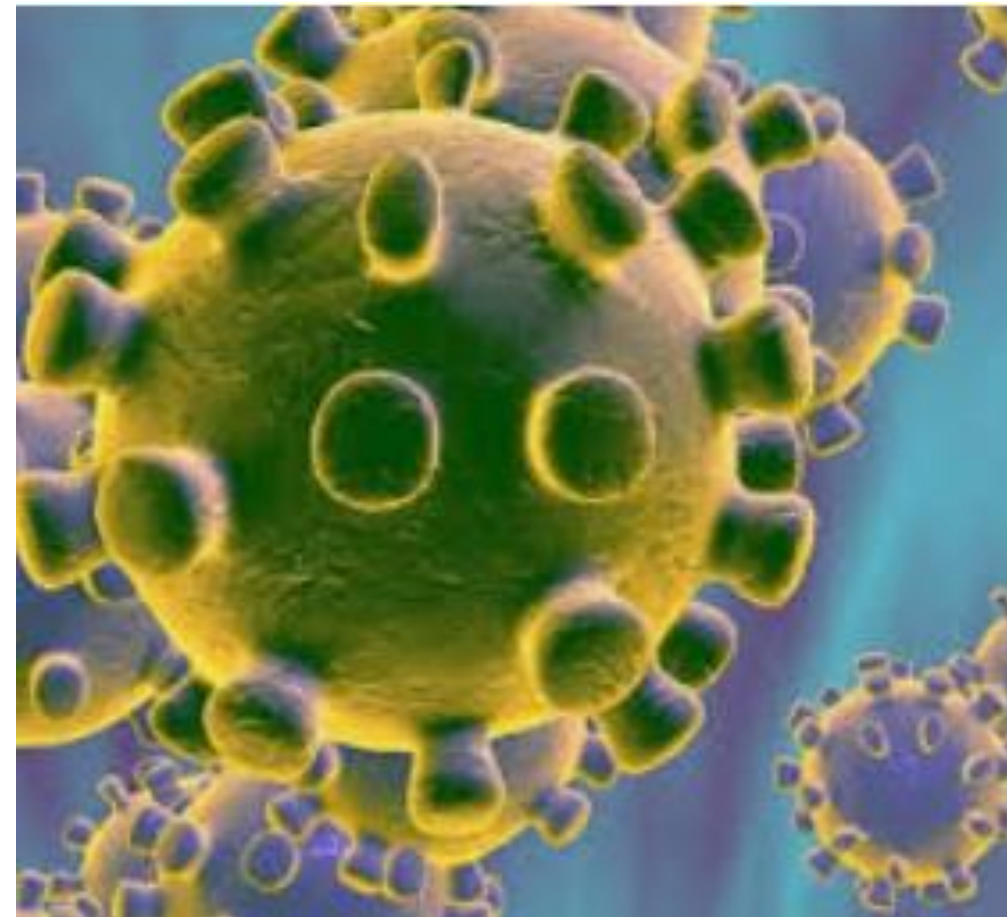
1. The Belgian DPA

2. Opinions of our Knowledge Center

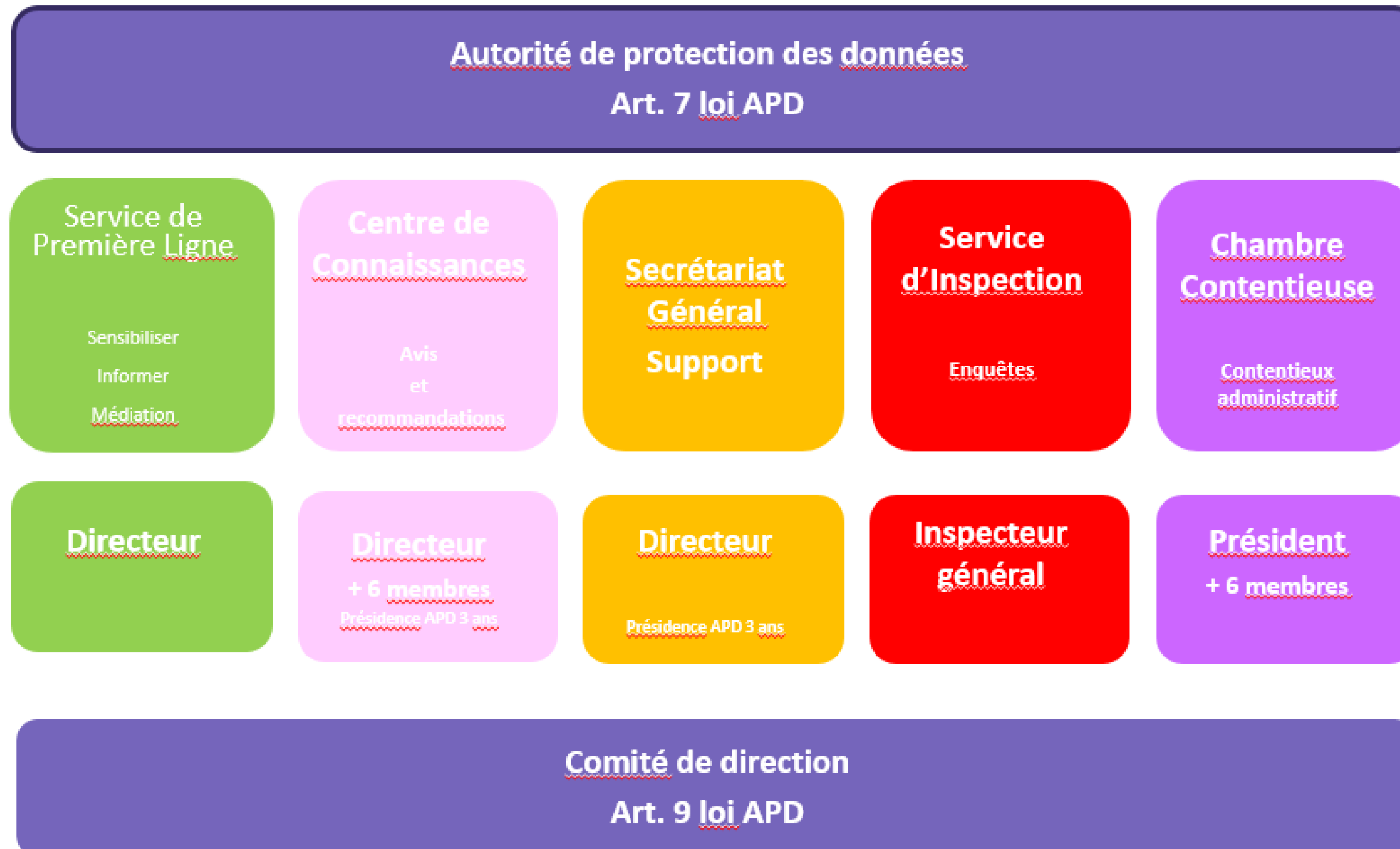
- Working and figures
- Scope of our analysis
- Corona-related opinions
- Non requested opinions

3. Other interventions of our DPA

- Advisory:
 - Opinion on Coronalert DPIA
 - FAQ's (website): horeca, temperature, municipalities
- Contentious
 - Complaints handling
 - No *ex officio* enquiries
 - Questions (airport + horeca)
 - Thermic cameras cases (Belgian coast)
- Appeals (1 before Council of State 1)



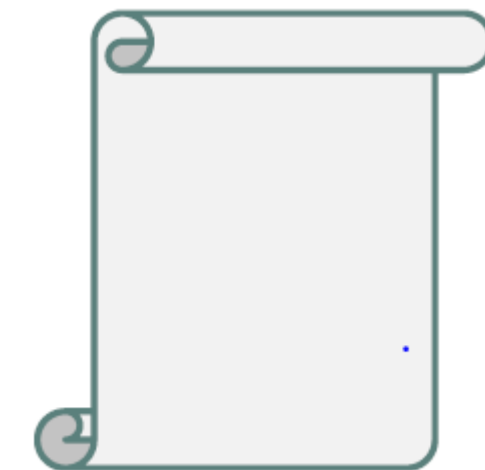
The Belgian DPA



Opinions of the Knowledge center: working and figures

Working and figures

- 1 Director + 6 external members (experts – appointed by federal parliament) - (+ staff) - hearings
- Art 36.4 GDPR + art 23 APD law (loi du 3/12/2017 wet)
- Opinions (requests by parliaments & governments) – laws and regulations
- Mandatory but non binding (// Council of State) – 60 (or 15) days
- Published on our website
- 150 – 300/year – usually followed...
- 32 advices on “corona “ draft bills and regulations



Opinions of the Knowledge center : scope of our analysis

I. Principles of legality and previsibility

- ❑ The right to data protection is a fundamental right
- ❑ Fundamental rights may be restricted – under certain requirements: necessary in a democratic society and foreseen by law
- ❑ Processing of personal data is a restriction to such fundamental right
- ❑ Processing of citizen's personal data by State entities should hence comply with certain rules
 - Processing of citizens personal data by State entities should be foreseen by a law
 - Essential elements (purposes, controller categories of data and persons, retention duration and transfers) of such processing should be defined
 - where important interference into citizen's right to data protection : in a formal law
 - where low interference into citizen's right to data protection:
 - purpose(s) and controller: in a formal law
 - other essential elements: in a formal law or in a execution act of the Gouvernement, provided that mandated to so in a formal law (+ clear and complete mandate)



II. Principles of necessity and proportionality (to achieve goal + no less intrusive means exist)



III. Others



Opinions of the Knowledge center

Corona-related opinions

- Sensitive: tracing, testing, vaccination, PLF data exchange and control
- Others: primes and subsidies, work dispense, videoconference

Corona-related bills and regulations for which no opinion was requested

- Horeca data gathering
- AM/MB 12/1/2021
- Dutch decrees and regulations



Opinions on contact tracing related bills

- +/- DPA Knowledge center advices so far (see DPA website under themes – Covid)
- Special powers Royal Decrees, draft bills, cooperation agreements, execution cooperation agreements, approval bills & decrees etc
- Tracing, which implies restrictions to data protection right, was first organized by Royal Decrees - Then translated into cooperation agreements (Council of State):
- Main issues
 - lack of clarity as to purposes + which data will be used by whom for which (of the 3 apparent) purposes (black-box)
 - Unjustified data centralization + possible links with other databases (undefined processing)
 - Use of data for research purposes reserved to given researchers - decisions by a “Committee” (CSI/IVC)
 - Disproportionate collection of personal data (not required for tracing purposes)
 - Health data (lung scans) not required for tracing purposes
 - Social security/ national number not required for tracing purposes + giving rise to unforeseen further uses/cross-uses
 - Undefined “additional data “



Opinions on vaccination related bills

▪ Law of 22 december 2020 (on antigenic tests)

- One single article
- Full delegation of powers to Government
- No opinion requested from Council of State and DPA

▪ Royal decree of 24 December 2020

- Two databases
- Codes database (priorities and invitations): data sources? Data categories?
- Vaccinated people database:
 - Vague purposes (much too broad or even illegible)
 - No link between data and purposes
 - Necessity and proportionality test hence impossible
 - Anonymised data not contemplated
 - CSI/IVC appointed to autorise data transfers to “public instances” – whatfor?
 - Retention duration: 2 years (“temporary crisis measure”)

▪ Cooperation agreement

- A few improvements (clarifications)
- Purposes still vague (ex: art 9.2h GDPR)
- CSI/IVC still designated to authorize data communicaions to third parties (withn vague purposes)

➤ Risks: re-use of data for other (non contemplated purposes)



Opinion on so-called “pandemic” law

▪ **Breach of legality principle**

- None of the essential elements are defined exhaustively (“notamment”)
- Excepted the purposes (“controle and surveillance of administrative measures”) but no definition of the data processing > no foreseeability
- Full delegation to the Government
- Possible re-use of all existing database held by State services (“compatible use”)

▪ **Breach of necessity and proportionality principles**

- No demonstration/analysis of the necessity of the (non defined) measures , nor (hence) of the data processing
- Proportionality test impossible to carry out given the lack of exhaustive definition of the data/data subjects/processing

▪ **Breach of transparency and previsibility principles**

▪ **Suggestions**

- A law framing measures and data processing which we believe we will have to put in place (again)
- + a procedural law whereby lawmakers and advisory bodies are imposed short timeframes to proceed (and where the parliament remains a deciding body – not a “a posteriori validator”)



Consequences and risks

- Mandatory registration of massive sensitive data
- In central database (necessary?)
- Unclear/vague/non-specific purposes lacking transparency (citizens+ parliaments) and leaving the door open to...
- Possible re-uses (+ datamining and matching) of data(bases) by State entities, without any parliamentary control (CSI/IVC, services integrators, broad interprétation of “only law”) etc - in line with current trends/deviance
- Risks unknown today but genuine and serious
- Enhanced data security risks (hacking) – linked to # of data and centralisation
- Lack of transparency



examples:

- Covid tests results : recommandations
> police controle and fines
- Covid tests results and vaccinal status:
passport/certificate



The logo for SCHOUUPS features a large, light purple hexagon with a white rectangular box in the center containing the word "SCHOUUPS" in a dark blue, serif font. To the right of this hexagon is another light purple hexagon containing a portrait of Sara Cockx. The background is white with several other light purple hexagons of varying sizes and orientations scattered around.

SCHOUUPS



Sara Cockx
Partner

“Things should be made as simple as possible, but not simpler”

Albert Einstein

**DATA PROTECTION IN CORONA TIMES
HR PERSPECTIVE**

CYBER SECURITY COALITION

25 MAY 2021

Sara Cockx,
Partner at Schoups

With the collaboration of **Kiandro Lebon**

SCHOUPS

INTRODUCTION: COVID IN THE WORKPLACE



- Field of tension
- Covid and Data Protection : main principles
- Some HR Covid classics
 - Covid-related (holiday) questions
 - Temperature measurements
 - Dealing with employees who are ill
- Current challenges
 - Compulsory vaccination
 - Vaccination questionnaires/passport
 - Teleworking from a distance/holiday home
- Future challenges
 - Differential treatment non-vaccinated employees
 - Smart offices
- Conclusion

I. FIELD OF TENSION



Employment and Welfare Obligations

- General duty of care for both the employer and the employee(s)
- Welfare Act and Codex with broad and strict obligations
- Supervision by FPS Employment
- Sanctioned with important criminal or administrative penalties



Data Protection

- Applicable to all measures involving the processing of personal data
- Strict interpretation by Belgian DPA, especially for health data
- Dispute Resolution Chamber: wide range of possible sanctions

irreconcilable field of tension?

Coronavirus

Familie van aan corona overleden Colruyt-medewerker dient klacht in



Beeld Thomas Sweertvaegher

De familie van Mohammed Nahi, de 32-jarige Colruyt-bediende uit Vorst die overleed aan de gevolgen van het coronavirus, heeft klacht ingediend bij het Brusselse parket. De familie verwijt de supermarktketen dat ze nalatig is geweest in het beschermen van haar personeel.

BELGA 25 juni 2020, 18:17

Privacywaakhond blijft erbij: "Contactopsporing is inbreuk op privacy, nu het wettelijk kader bekijken"

De Gegevensbeschermingsautoriteit, de vroegere privacycommissie, blijft erbij: de contactopsporing die moet uitzoeken met welke mensen besmette personen contact hadden, is een inbreuk op de privacy. De commissie bekijkt of de wet moet worden aangepast. Doorvragen naar de locatie bij contactopsporing is geen probleem voor de Gegevensbeschermingsautoriteit.

DATA PROTECTION

“Public health is of paramount importance to us.

*Prevention and the right to personal data protection
are not contradictory.*

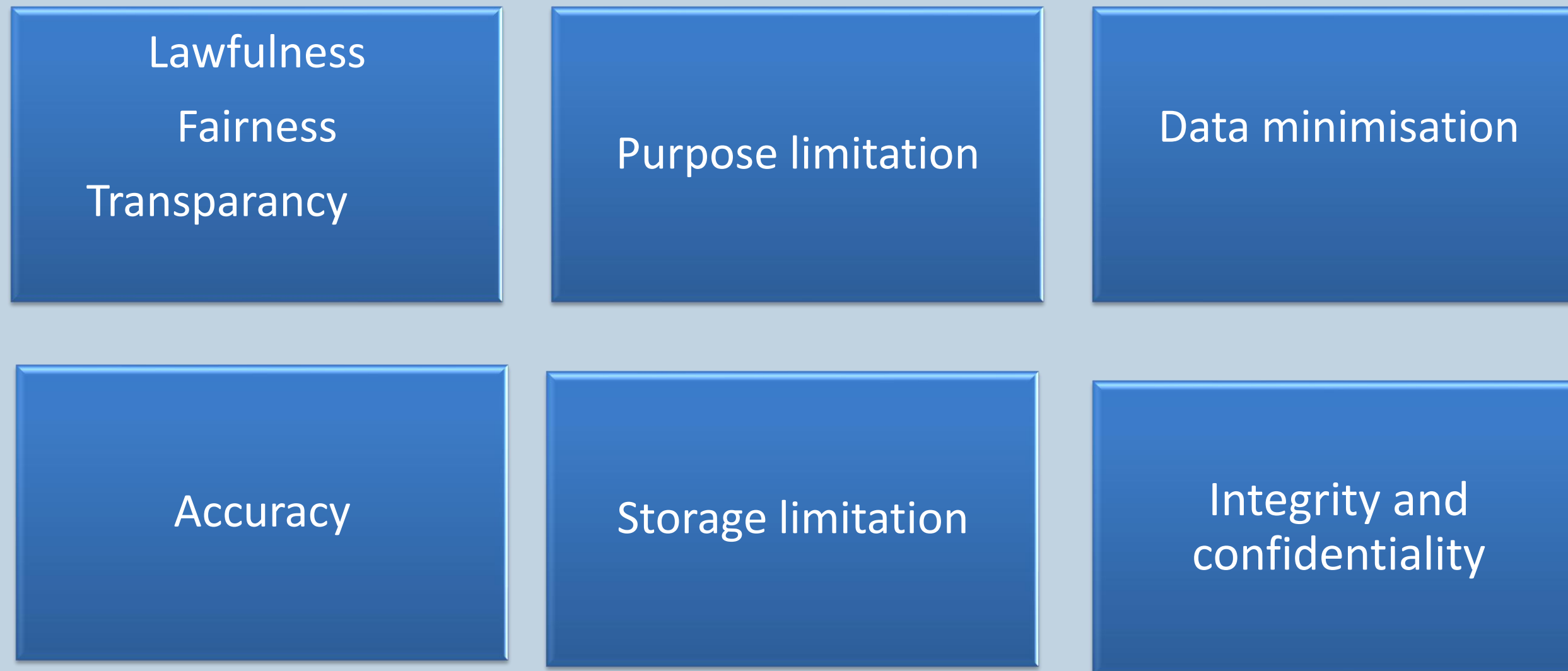
*We do recommend, however, that you follow the
instructions of the competent authorities - including
the FPS Public Health - so that all measures taken are
proportionate.*

*This will ensure both good **hygiene in life as well as in
data**”*

*- Belgian Data Protection Authority
(translation)*

II. COVID AND DATA PROTECTION

- (Preventive) measures involving the processing of personal data
- General principles relating to processing of personal data (art. 5)



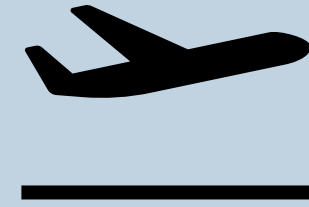
II. COVID AND DATA PROTECTION:

- Lawfulness of processing
 - Protection vital interests?
- Data concerning health
 - Principle: processing is prohibited
 - Exceptions subject to restrictive (lawfulness) requirements

II. COVID AND DATA PROTECTION:

- Possible grounds within an HR-covid-context
 - **Explicit consent** of employee (9,2, a)
 - DPA: *“Not possible due to subordinate relationship”*
Quid general labour law practice & Dispute Chamber’s Decision of 9 November 2020?
 - Necessary to carry out the **obligations in the field of employment law** (9,2, b)
 - In so far as it is authorised by Union or Member State law
 - DPA: *“General duty of care is insufficiently precise”*
 - Quid detailed obligations under the welfare legislation?
 - Necessary for reasons of **public interest in the area of public health** (9,2, i)
 - DPA: *“Only if employers act in implementation of explicit directives imposed by competent authorities.”*

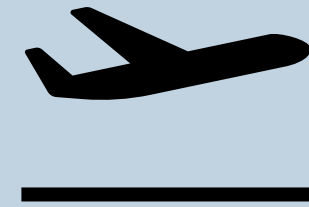
III. SOME HR COVID CLASSICS



COVID-RELATED QUESTIONNAIRES

- Mandatory **questionnaires** on:
 - holiday destination
 - disease symptoms
 - high-risk contacts
- = in principle not allowed
- Quid mandatory welfare risk assessment (well-being policy in the workplace)?
- Quid mere information about holiday destination? Is this also data concerning health?
- DPA: allowed as the employee or visitor can **freely refuse without suffering any negative consequences.**
 - Implicit recognition that employees can sometimes give consent?

III. SOME HR COVID CLASSICS



COVID-RELATED QUESTIONNAIRES

Our advice:

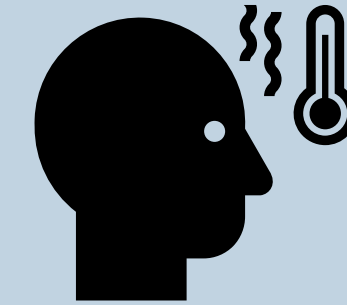
- Make your employees aware of their own legal obligations and responsibilities

- Employment Contracts Act + Welfare Act
 - Obligation to comply with (safety) instructions
 - Prohibition to harm themselves, colleagues and third parties
 - New Art. 238 Social Criminal Code: every person's own criminal liability to comply with Covid measures

- Encourage them to provide you with the information voluntarily

- Consult your prevention advisor-occupational physician (Royal Decree of 5 January 2021)

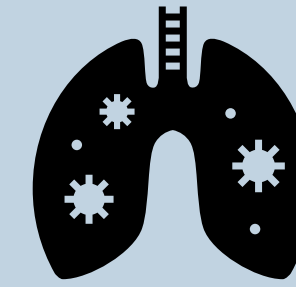
III. SOME HR COVID CLASSICS



TEMPERATURE MEASUREMENTS

- Effectiveness: questionable
- FPS Employment : exceptionally allowed under strict conditions CBA n° 100 (alcohol/drugs)
- DPA: strict position - in absence of specific legal ground - not allowed to:
 - take temperature of individuals and record the results in a file.
 - take temperature with the aid of advanced electronic measuring devices such as fever scanners, heat cameras or other automated systems
- But: **GDPR does not apply if temperature or other data are not registered**
- Wellfare Codex and Health Care Act only allow medical acts under strict conditions

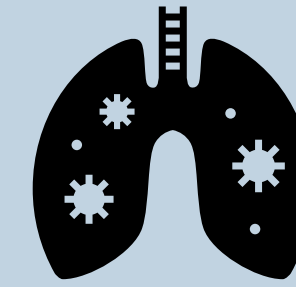
III. SOME HR COVID CLASSICS



DEALING WITH EMPLOYEES WHO ARE ILL

- Mandatory Covid tests = not allowed
 - voluntary self-tests?
- FPS Employment : ill employees can be sent home and asked to consult their doctor
- DPA: No obligation for employees to inform employer about symptoms/infection
 - The duty of care towards colleagues would not affect this
 - Voluntary reporting possible
 - Employer can ask to consult a doctor (no obligation)

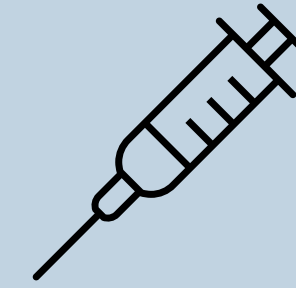
III. SOME HR COVID CLASSICS



DEALING WITH EMPLOYEES WHO ARE ILL

- Can an employer **disclose the name of an infected employee?**
 - No
 - Except if the employee has disclosed it himself
 - “data which is manifestly made public” (art. 9, 2, e)
- Important role of the prevention advisor-occupational doctor (new competences)
- Data protection concerns disproportionate to the work and welfare obligations?

IV. CURRENT CHALLENGES



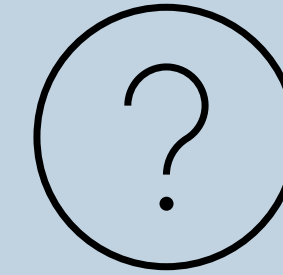
MANDATORY VACCINATION?

- No, vaccination cannot be mandatory
 - **Free choice** whether or not to get vaccinated (ECHR – Patient Rights Act)
 - FPS Employment & DPA: same position
- Freedom is not absolute, statutory exceptions are possible
 - Currently not in Belgium

Our advice:

- Inform your employees about facts and benefits of vaccination
- Raise awareness on own protection as well as the protection of others

IV. CURRENT CHALLENGES



VACCINATION QUESTIONNAIRES?

- Requesting this information = prohibited processing of health data
- Employee cannot be obliged not inform employer
- DPA: No legal ground - employee's consent cannot be invoked
 - Too strict? What if it is certain that there are no disadvantage in case of refusal to inform? What if made public information?
 - Quid strict welfare obligations and necessity to carry out in the field of employment law (9,2, b)?
- DPA: Occupational doctor cannot inform the employer (professional secrecy)

IV. CURRENT CHALLENGES



TELEWORKING FROM ABROAD / HOLIDAY HOME

- Employee must inform employer
 - Employer is entitled to know where the employee will work
 - Obligatory mention in the individual agreement on structural telework
- To do:
 - Clear policy/agreement on expected availability
 - Check occupational accident insurance
 - Written document stating where you working is necessary to benefit from legal presumption(s)
- Possible social security issues – medical assistance – hospitalization
 - Solution: (European) posting – A1 and other formalities
- Outside EUR → international data transfer!

V. FUTURE CHALLENGES

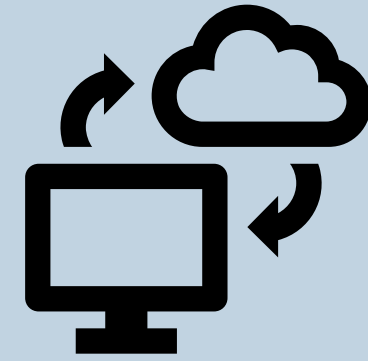


DIFFERENTIAL TREATMENT NON-VACCINATED EMPLOYEES

- Discrimination on the basis of health Data = not allowed (Discrimination Act)
- FPS Employment: **not** allowed to :
 - Reward employees who have been vaccinated
 - Possible: collective bonus (CBA n°90) in function of level of absenteeism
 - Sanction or deny certain benefits to those who have refused to be vaccinated
- Corona measures remain mandatory for all employees
 - [generic guides](#), ministerial decree, ...
- Future: vaccination passport as basis or different treatment?
 - Clear statutory basis required
 - Proportionality of measures must be kept in mind

V. FUTURE CHALLENGES:

SMART OFFICES



- Processing of office data and presence of employees
- Lawfulness of processing ?
 - Performance of the (employment) contract
 - Legitimate interests of the employer
- Software – service providers = processor
 - Important: work with a reliable processor + processing agreement
- Information-consultation of works council / trade union delegation
- If time registration is included → mandatory provisions in the work regulations
- Use of cameras → CBA n° 68 to be complied with

CONCLUSION



SCHOUPS

CONCLUSION

- Welfare obligations and protection of personal data
 - = difficult to reconcile, but not impossible
- Legal initiatives required
- DPA's strict position is understandable but sometimes seems to overlook labour or welfare obligations
- Very important: raising awareness and accountability with the employees

QUESTIONS?



SCHOUPS

WWW.SCHOUPS.BE

S C H O U P S



Prof. Dr. Paul De Hert

BRUSSELS 25 May 2021

How do data protection rights fare in Corona times?

Professor Paul De Hert

Vrije Universiteit Brussels – University of Tilburg

general

- The discussion on the Covid tracing-app was a golden one for the data protection community, since it allowed to do the things we like to do: checking on legality and appropriate safeguards. Data protection is at its strongest when it transplants a discussion in favor or against a technology by a discussion on the kind of design and (further) use of a technology.
- It reminded me about the body scanner discussion in the late 2000's and how a sensible application of data protection principles and rules made a difference between overprotected badly designed body scanners and transparent and compliant scanners.

BUT

BUT SOME FALLACIES

- Technologies that are malum in se as opposed to male prohibitum (face recognition)
- Governments do not allow the 'data protection exercise' OR broader rule of law discussion (political urgency)
- Data Protection authorities do not do the 'data protection exercise' properly because of political pressure
- Data Protection authorities are at drift in the 'data protection exercise' uneasy with the underlying tension between fundamental rights that seem to clash (health, security, etc)
- Data Protection authorities are at drift in the 'data protection exercise' because apparently the GDPR seems to make good government impossible
- The 'data protection exercise' cannot be done properly since the legal framework gives a free pass to government (or private firms)

The exercise today ?

- Run all possible examples through the list of phallacies on the previoius slide and make carefull assessment of every measure
- Eg the contact centers, the passenger location form, the Corona App, temperature measurement, the pandemic act, drone use by local police, police measures to limit freedom of movement (1km, stop and search ...)..
- Caveat: need for multiactor/level analysis
 - we had two governments with different players; categorical judgements will not be instructive for our exercise today: the app under Philippe De Backer (GDPR proof expert) and the police measures under Pieter De Crem (expert of what?)
 - But the multilevel analysis needs to be broader:
 - Interplay federal regional *and* local actors (jumping of scales)
 - Interplay EU level and Member State level (jumping of scales and agenda blending)

Elements of discussion

- Pandemic Act proposal back to Council of State (DM 21 May 2021)
- Eu health certificate from July 1 (freedom of movement, as a rule no additional member state limits, alternatives to vaccination...) (DM, 21 May 2021),
 - but further use in MS? (France, not in restaurants April 20)
 - legal basis (connecting 'traçage' et 'vaccination') role Comité de sécurité de l'information
- <https://ai-regulation.com/the-french-government-permits-automated-video-surveillance-of-mask-wearing-on-public-transport-following-authorisation-by-the-cnil/>
- According to the Belgian Supervisory Body for Police Information it is not function creep that CCTV installed for counter-terror measures is now being used to control corona measures & it is perfectly in accordance with the law as the police can use cameras for whatever they like for crime control the purpose seems to be irrelevant.

<https://www.tijd.be/politiek-economie/belgie/algemeen/antwerpse-politie-mag-bewakingscamera-s-in-joodse-wijk-inzetten-tegen-corona-inbreuken/10294547.html>

Broader reflection COVID-19, a stress test for democracy and regulation and governance of data

- Legal architecture of dplaw in Belgium: la loi créant le CSI
- Legal architecture of surveillance law in Belgium: Loi Jambon CCTV & data retention law
- Technological surveillance architecture: data retention infrastructure has been embedded & ANPR and intrusive CCTV (all but facial) too

How was this possible?

-depolitising via technocratic governance

-substantial criticisms regarding the GDPR: 1) technocratic blurring language 2) the role of the data controller is so central that any decision whether to involve citizens remains in their hands.