Summary of the workshop and of the survey

European Civil Society Workshop on the Compensation of Data Protection Harms

Contact information:
julien.rossi@utc.fr
lucien.castex@isoc.fr

Background information

The European Civil Society Workshop on the Compensation of Data Protection Harms took place in Paris, on April 25th, 2018 [1]. It was made possible thanks to the support of Internet Society France. Participants were academics, lawyers and NGO members from France, Belgium, the Netherlands, Poland and the United Kingdom. The aim was to share experiences useful for the implementation of article 80 GDPR, and discuss the new possibilities it offers to enforce data protection rights of individuals in Europe, and the challenges faced, taking into account the challenge posed by the evaluation of harm caused by infringements to data protection law.
This document presents a short summary of findings.

Summary of the discussions

The workshop was divided in three even parts :

- First participants had 10 minutes to present their research or projects with regards to art. 80 GDPR ;
- Then we discussed the results of the survey ;
- And finally we debated strategies on how to compensate harm to data subjects caused by an infringement on their right to the protection of personal data.

Participants to the workshop

- **Lucien Castex**, ISOC France and Université Sorbonne Nouvelle
- **Gloria González Fuster**, research professor at the Vrije Universiteit Brussel
- **Karolina Iwańska**, Fundacja Panoptykon
- **David Martin**, Bureau européen des unions de consommateurs (BEUC)
- **Nick McAleenan**, lawyer in charge of the Morrisons case, JMW Solicitors LLP, Manchester (UK)
- **Athur Messaud** and **Alexis Fitzjean O'Cobhthaigh,** from la Quadrature du Net
- **Laura Vael**, lawyer taking part in the E-Bastille initiative
- **Julien Rossi**, researcher at the Université de technologie de Compiègne
- **Tim Walree**, researcher at the Radbourd Universiteit in Nijmegen

A concern raised by La Quadrature du Net is that suing unlawful data controllers in civil courts for financial compensation in cases where the violation of data protection rights is still ongoing will end up setting a price for unlawful processing of personal data. For example, if the amount of compensation is 10€ per data subject in a given country for the simple violation of data protection rules, such as the validity of consent under art. 6 GDPR, then this will in effect the « price » of this data. Nevertheless, many other participants voiced the importance of allowing data subjects to get compensation for the individual harm they suffered. Collective redress mechanisms were seen as ways to guarantee that, but also to financially incenticise data controllers to comply with the law. This led to a discussion on the underlying philosophy of data protection as either a coherent fundamental

right in itself for the individual, based on informational self-determination, or rather a collective right that protects other individual rights.

One other issue of debate was on what would qualify as harm.

Indeed, a lot of bad things can happen to data subjects whose personal data have been unlawfully processed, such as identity theft, or even physical threats if, for example, their adress is disclosed to terrorists, as had happened in one of the cases mentioned in a survey answer. But often, it is for the data subject very hard to know when his or her personal data is being unlawfully processed, and even harder to pinpoint damage that was caused by this unlawful behaviour of the data controller.

Given the few cases in which individual data subjects have been awarded civil compensation for harms related to their personal data, it is also very hard to estimate the benefits of litigating in civil courts, given the relatively high cost of such a procedure. This is where collective action and the role of NGO's come into play.

Yet while it is possible to look at all the aspects of a case and find out how one person was harmed, for example, by unlawful disclosure of personal data or by the refusal to rectify false data held on him (like financial or taxation related data), it is quite hard to do so on the scale of the many litigants of a collective action. For example, if payroll data is leaked, associated with the adress of the person, and that the account of a person being paid quite well is robbed as a consequence of the information disclosed by the leak, then there is material damage that can be assessed for this person, but not for the others. Another person may have suffered immaterial damage to his or her reputation because of the same leak, but others may not.

There appears to be, however, a general trend towards recognising immaterial damages in civil courts more and more easily. And the GDPR does provide for the possibility to get compensation for immaterial damage, so even in countries where case law does not easily recognise this, referals to the ECJ to interpret this notion of immaterial damage in the GDPR may lead to changes at least in this area.

Although collective action projects by NGO's do not always seek compensation, whether for political, practical reasons or due to national procedures not allowing this, they may still ask for an injonction to cease the act leading to the damage. The judge can then set a penalty for delay in compliance with this injunction. And as the injunction would often hurt the financial interests of companies that NGO's want to litigate against for strategic reasons, this will still give them a financial incentive to comply with the GDPR even despite the fact that financial compensation may or may not be granted to the data subjects involved in the collective action.

Finally, we discussed the cross-border aspects of art. 80 GDPR. How does it combine with the one-stop-shop and consistency mechanisms in cases where NGO's bring cases to a national DPA ? What happens when a data subject in country A gives a mandate to an NGO based in country B to litigate against a company whose main establishment is in country C ? Do national procedural laws allow this ? How does this combine with the Brussels and Rome regulations ? These questions were evoked but we did not have time to go much further into them, and further work (or practice) will be needed to find answers to these questions.

Summary of the survey's findings

There were less answers than expected (only 4 received so far). So it is difficult to figure out a comprehensive picture of the implementation of article 80 and article 80 in conjunction with article 82 GDPR across Europe.

There does appear to be a general trend towards allowing NGO's to represent data subjects' interests to a certain extent, and also to claim compensation. Obstacles may vary according to some procedural limitations set into national law. For example, in some countries, NGO's may only act if mandated by data subjects, whereas in France, an NGO may act on its own. Also, there may be differences between the liability of public and of private persons.

With regards to the compensation of harms related to data protection when the case was brought by an individual, there does not appear to be a fixed method yet for the determination of the amount of financial compensation, except in the UK where there are some general guidelines in cases of unlawful disclosure of private information (which may also be personal data).

The amount that is awarded varies according to the court, but also depending on the nature of the infringenment. In the Netherlands, one exceptional judgement awarded € 100 for the compensation of the non-material damage caused by a simple infringement of data protection law by an insolvency register. In Austria and in the United Kingdom, similar infringements led to awards of respectively 750 euros (in Austria) and pounds (in the UK).

In some other cases, where significant distress happened, for example because of identity theft leading to the data subject being sent tax claims based on falsified data, and where he or she could not exercise his or her data protection rights to rectify the situation, higher amounts have been awarded. For example, the ECtHR awarded a € 9000 compensation in the « Romet vs. Netherlands » case.

In other countries, like France, individual claims for distress due to infringement to data protection rights seem harder to obtain.

If we follow the general trend of the amounts of financial compensation awarded to data subjects in cases of individual claims, then it appears that a baseline of €100 per « basic » infringement seems a reasonable expectation. NOYB, a Vienna-based NGO, is preparing a lawsuit against Facebook claiming €500 compensation per data subject whose rights have been infringed. There were about 25 000 signatories in the claim, so this would amount to a total « fine » of 12 500 000 euros.

However, if, in France, an NGO representing all of the French users of Facebook (about 32 million people according to Statista), and claiming a token amount of €1 per data subject, could cost Facebook up to 32 million euros, or even 3,2 billion euros if the (unlikely) baseline €100 per data subject value is taken into account.

A practical question that may arise is: will the amount of compensation that a data subject can claim differ depending on whether he or she brought the case herself in front of the courts, or whether he or she was represented by an NGO in a collective redress lawsuit, due to economic considerations?

State of implementation of articles 80 and 82 GDPR

Jurisdiction	Art. 80 §1	Art. 80 §2	Art. 80 + Art. 82
France	Will have direct effect	art. 91 loi Justice au XXI siècle Only concerns the cessation of the infringement for now, should also include compensation under the new Data Protection Act	Collective redress (with compensation) should become possible under the new Data Protection Act implementing GDPR
Austria	Implemented	Not implemented, but should be implemented soon (new DP Act)	Implemented
Poland	→ Possibilities are open in front of administrative courts (some conditions apply) → Possibilities to represent data subjects in front of the DPA → Not in front of civil courts	→ Enter proceedings before the DPA at any stage as a third-party intervener → Present an *amicus curiæ* → Demand the initiation of proceedings at the DPA even without a mandate	Compensation will be only on an individual basis (once the GDPR is implemented). Compensation for both material and non-material damage.
Netherlands	No implementation needed (monistic system) Possible under art. 3:305a of the Civil Code (*Burgerlijk Wetboek*) Only concerns the cessation of the infringement (*gebodsactie*)	Implemented by art. 1:2 section 3 of the General Administrative Act (*Algemene wet bestuursrecht*) and art. 3:305a of the Civil Code (*Burgerlijk Wetboek*)	Under the Civil Code : the representative entity cannot ask for compensation. But it can under the Collective Settlements Act 2005, used only 7 times so far. « It is likely that in the near future the prohibition on collective claim of damages no longer exists » (see : Wetsvoorstel Afwikkeling Massaschade in een Collectieve Actie)
United Kingdom	Sections 180-182 DPA Bill → Data subjects can mandate an NGO to exercise rights to lodge complaints and to an effective judicial remedy → Class actions are only possible with the data subject's consent (opt-in)	Not yet (but could be introduced by Regulation as provided under the discussed Data Protection Act Bill)	→ Section 180 of the proposed DPA Bill allows NGOs to bring compensation claims to court on behalf of data subjects → See also section 13(1) of the DPA Act 1998 and Vidal-Hall case

→ Note that in some countries (e.g. France), art. 80 GDPR is going to be implemented by pre-existing measures in national law

Obstacles

Nick McAleenan (JMW) - United Kingdom

- There are a limited number of NGO's genuinely concerned with data protection;
- How will data subjects become aware that their rights have been infringed ? How will they be motivated to join ?
- Funding : can NGO's sustain a class action ?There were less answers than expected (only 4 received so far). So it is difficult to figure out a comprehensive picture of the implementation of article 80 and article 80 in conjunction with article 82 GDPR across Europe.

Strategies to circumvent obstacles

Poland (Fundacja Panoptykon): « In practice, in some cases this difficulty can be overcome by engaging individual employees of the NGOs as data subjects, thus making it possible for NGOs to represent them in proceedings before the DPA. This is a limited option, because in some cases data processing involves particular categories of subjects, e.g. when it comes to data processed in the workplace or as part of specific services […]. In such cases NGOs will still be able to initiate proceedings in particular cases before the DPA and administrative courts […]. »

Cross-border reach

As pointed out by Fundacja Panoptykon, « NGOs' engagement in the exercise of the rights of data subjects based in another Member State […] necessarily means that the NGO will have to possess enough expertise in the member state's procedural law. This is a challenge difficult to overcome especially for small organisations »

Also : « Some member states may also limit the possibility to exercise the rights of data subjects to organisations registered in that member state » (Fundacja Panoptykon)

In the Netherlands (Tim Walree - Radboud Universiteit)

There is a law proposal stating that NGO's can claim damages from a party if there is sufficiently close connection with the Dutch juridiction. There is possibility to claim damages in the name of data subjects who are not in the Netherlands, but in another member state, but they will have to opt in to the class action specifically.

In the United Kingdom (Nick McAleenan)

Under the UK's « new » Data Protection legislation, controllers and processors established in the UK or those established outside of the UK but who offer goods and/or services to data subjects in the UK will be covered. The new law therefore ties the defendant and claimant closely to the UK. Also, Article 80 states that an NGO must be 'properly constituted' in the member state where it is seeking to bring the collective action.

There is a link with the Brussels Regulation (1215/2012). Defendants should be sued where they are domiciliated, but tort proceedings like a breach of the GDPR can be brought where the harm occured.

Recital 144 GDPR : if a court is informed that a case is pending in another member state it must check and verify the fact and proceedings may be suspended.

Controllers and processors established outside the UK but providing goods and/or services in the UK will be covered by the DPA Bill, so action against them should be possible.

Lawsuits initiated by NGO's		
Jurisdiction	**Before the GDPR**	**After the GDPR (projects)**
Poland	No	« After the GDPR becomes fully enforceable, we are planning to involve in litigation concerning **access rights** of individuals to their data »
Netherlands	Only lawsuits against some unlawful acts (data retention and surveillance legislation), by organisations such as Bits of Freedom and Privacy First	
France		E-Bastille by ISOC France, based on the national class action procedure, suing for compensation LQDN is using art. 80 GDPR to bring Google, Facebook, Amazon, Apple and Microsoft to the French DPA, not suing for compensation

Proposed methods to evaluate the amount of compensation to be asked

Poland (Fundacja Panoptykon)

At the moment, it is not possible to claim compensation. There is no precedent, but « some inspiration can perhaps be drawn from existing case law on harm evaluation in other areas of law, especially related to personal rights (e.g. defamation) »

Austria (NOYB.eu)

« For the "class action" against Facebook in Austria we asked for a "token amount" of € 500 per data subject, but we're confident we could have asked much more »

There was a precedent with a decision by the Austrian Supreme Court (OGH 6 Ob 247/08d) : 750 € for a wrong entry in a credit rating database, which harmed the reputation of the data subject.

Netherlands (Tim Walree - Radboud Universiteit)
Damage can be material or immaterial

"There is no general method to evaluate immaterial damages. The civil judge has the competence to estimate the amont of damage, if the extent of the damage cannot be determined accurately […]. In the Netherlands, some judges use the "ANWB Smartengeldgids". This is a reference work with judgments for the determination of the amont of immaterial damages. There are no references with regard to data protection harms" (Tim Walree)

There are some precedents :

- « X/Advocatenkantoor » : 100 € for a data subject, concerning a company that collected data from an insolvency register unlawfully and sent a letter to a data subject offering its services ;
- « Van Hees/X » : the data subject's data was misused by a fraud (identity fraud case) and subsequently received tax assessments and claims from government authorities. The data subject was awarded 1000 € as compensation

- « X/agis » : an insurer unlawfully provided confidential data address of a former wife to a violent former husband : 2500 € were awarded for compensation of the fear

- ECtHR « Romet vs. Netherlands » : failure by government authorities to rectify data held on the data subject in the vehicle register : 9000 € awarded by the ECtHR (there had been significant distress caused by the amont of tax claims received based on the registration of over 1000 vehicles under his name using a driving licence stolen in 1995)

Simple violation of data protection law :

- 100€ awarded in a Dutch case
- 9000 € awarded by the ECtHR
- In the other cases, a moderate level of compensation is granted if three criteria are met : severe violation, extraordinary consequences, exceptional circumstances.

United Kingdom (Nick McAleenan - JMW)

There is some precedent, mostly with individual cases, regarding general breaches of data protection :

- English Court of Appeal, case Vidal v. Google [2015] : there can be compensation without pecuniary loss for the breach of the Data Protection Act 1998

- Halliday v. Creation Consumer Finance Ltd [2013] : £750 « for distress in a case of an inaccurate credit reference » (Note : a similar amount to what was awarded in Austria in a similar case)

- Grinyer v. Plymouth Hospital NHS Trust [2011] : £12,500 for « significant exacerbation of an existing medial condition caused by unauthorised disclosure of medical information »
- AB v. Ministry of Justice [2014] : £1 for « delay in complying with a subject access request » and £2250 for distress

- CR19 v. Chief Constable of the Police Service of Northern Ireland [2014] : £1 nominal compensation for « breach of data subject rights » but also £20,000 under a negligence claim as the data had fallen into the hands of terrorists

Regarding private information/data disclosure cases:

- TLT v. Secretary of State for the Home Department [2016] : awards between £2500 and £12500 for the disclosure of data regarding asylum seekers

- Gulati v. MGN Limited [2015] (media phone-hacking), the court stated that the relevant factors to be taken into account were :
    - The subject matter and significance of intrusion
    - The effect on claimant
    - The effect of repeated intrusions can be cumulative (if relevant)
    - The extent of damage may be claimant specific

- Burrell v. Clifford [2016] : added the following criteria in the evaluation :
    - The nature of the information
    - The nature, extent and purpose of the misuse
    - The consequences of the misuse

  - Whether the misuse caused financial loss or provided financial gain to the wrongdoer
  - Any relevant policy factors (eg protection of rights of children)
  - Mitigating/aggravating factors

- Morrisons case, by JMW, on behalf of Morrisons' employees, is the first claim for collective redress (and not just an individual case). The case is run under a « Group Litigation Order ».

One has to be aware that a data controller may not be liable if « it proves that it is not in any way responsible for the event giving rise to the damage » (art. 82(3) GDPR) or if it can prove that « he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned » (section 13(3) Data Protection Act 1998)

On settlement

Most of those who answered the final question of the survey and all the participants in the workshop were of the opinion that settlement before precedent is created would be detrimental, at this point, for data protection.