

PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a publisher's version.

For additional information about this publication click this link.

<http://hdl.handle.net/2066/194516>

Please be advised that this information was generated on 2020-09-26 and may be subject to change.

THE CONTROL BY AND RIGHTS OF THE DATA SUBJECT UNDER THE GDPR

By **P.T.J. Wolters**

INTRODUCTION

The General Data Protection Regulation (GDPR) creates several obligations for “controllers” and “processors” of “personal data.”¹ The regulation replaced the “Data Protection Directive” and its national implementations on May 25, 2018.² It has been adopted to strengthen the protection of personal data.³ However, it will only lead to this result if the controllers and processors comply with their obligations. Under both the Data Protection Directive and the GDPR, enforcement largely depends on the national supervisory authorities. In practice, this supervision does not guarantee an effective protection of personal data.⁴ The GDPR empowers the “data subject” in order to improve this protection. It creates and strengthens several rights that grant him control over the “processing” of his personal data.⁵ This control allows him to better decide who is authorized to process his data and the purposes for which this is permitted.⁶

In this article, I will give an overview of these rights and analyze the extent to which the GDPR

truly strengthens the control by the data subject. I will answer the following research questions: *What are the rights of the data subject under the GDPR? To what extent do these rights strengthen the control over the processing of his personal data?* This article proceeds as follows. Section “The position of the data subject” describes the disadvantaged position that limits the control by the data subject. Next, sections “The right of access” through “Modalities in relation to the exercise of the rights of the data subject” give an overview of his rights and the rules in relation to the exercise of these rights. This overview contains a comparison between the GDPR

Continued on page 7

THE CONTROL BY AND RIGHTS OF THE DATA SUBJECT UNDER THE GDPR 1

By *P.T.J. Wolters*

CAN COMPANIES DISCLAIM AND LIMIT LIABILITY FOR DATA BREACHES IN ONLINE TERMS OF SERVICE? 3

By *Alex Pearce*

BIOMETRIC TECHNOLOGY: SECURITY AND PRIVACY CONCERNS 19

By *Robee Krishan and Reza Mostafavi*

P.T.J. (Pieter) Wolters is an assistant professor of private law at the Radboud University and a researcher at the Business and Law Research Centre. This article is an adaptation of a paper previously published in the *Tijdschrift voor Consumentenrecht & handelspraktijken*: “P.T.J. Wolters, ‘De rechten van de betrokkene onder de AVG’ [2018] *TvC* 130”.

The Control by and Rights from page 1

and the Data Protection Directive. I subsequently analyze the extent to which the GDPR strengthens the rights and the control by the data subject (section “Synthesis”). The article ends with a conclusion. Although the GDPR enhances the rights, it only leads to a limited strengthening of the control by the data subject (section “Conclusion”).

The scope of this article is limited in several ways. First, a controller has several obligations that exist independently of any action by the data subject. These duties create rights for the data subject. Indeed, he can enforce them pursuant to Article 79 of the GDPR. These rights and obligations are not covered in this article. For example, I do not discuss the “right to information at the collection of personal data” or the “right to data protection by default”.⁷ Instead, the article is limited to the rights contained in chapter III of the GDPR that only create legal obligations for the controller if the data subject actively chooses to exercise them. Furthermore, the discussion of the rights is limited to the aspects that are important for the answer to the research questions. An emphasis is put on elements that affect the control by the data subject and the differences between the GDPR and the Data Protection Directive. Finally, the article does not cover the limitations of the rights of the data subject pursuant to the interests mentioned in the Articles 23 and 89 of the GDPR and Article 13 of the Data Protection Directive.

THE POSITION OF THE DATA SUBJECT

The position of the data subject relative to the controller is weak. It can be compared with the relationship between a consumer and a business.⁸ A controller will usually process personal data in the course of its professional activities.⁹ It processes the data of a large group of data subjects¹⁰ in a standardized manner and has the required financial means, organizational capacity, and technical expertise. In contrast, the personal data of a single data subject are processed by many controllers and in many different ways.¹¹ A data subject is not practically able to maintain an overview of these controllers and processing operations.¹²

Furthermore, it can be difficult to establish the exact consequences of individual operations.¹³ Many Europeans feel that they have insufficient control over their personal data.¹⁴

The rights are aimed at improving the control by and the position of the data subject. However, this disadvantaged position can prevent him from effectively exercising his rights.¹⁵ For example, a data subject will not benefit from his right of access if he does not know the parties that might process his personal data or if he cannot value the provided information.¹⁶ The right to data portability will not improve his protection if the competitors of the controller process the personal data in the same manner.¹⁷ Furthermore, a violation of the GDPR frequently affects a large number of data subjects or even society as a whole. The enforcement through individual rights is at odds with this “collective nature” of data protection.¹⁸

In this respect, data protection law is different from consumer law. A consumer that is faced with unfair contractual terms or goods that are not in conformity with the contract of sale might not know his legal rights. However, he will at least know that he is adversely affected. For example, the consumer will know that he is stuck with an unwanted subscription or a broken telephone. This can induce him to look into his legal rights. In contrast, such a stimulus is absent if the data subject does not know that a bank is using incorrect personal data to deny a loan application without human intervention or if he does not know that these data are acquired from another controller that should have deleted the information a long time ago.¹⁹

RIGHT OF ACCESS

Pursuant to Article 15 of the GDPR, a data subject has the right to obtain from the controller confirmation as to whether or not his personal data are being processed. Article 15(3) grants the data subject the right to a copy of the processed data. Furthermore, the controller is obligated to provide information about this data and the processing operations. Pursuant to Article 12(1), this information should be presented in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

The right of access is a logical first step toward the exercise of the other rights. For example, a

data subject cannot effectively request a correction if he does not know what personal data are incorrect. For this reason, the provided information should enable the data subject to become aware of the data, to check that they are accurate and processed lawfully and to exercise his other rights.²⁰ However, the other rights are not limited to data subjects that have exercised their right of access.²¹ The data subjects can also exercise them if they become aware of the processing in another way. For example, if an insurance agent informs a customer that his insurance becomes more expensive because he has caused several accidents, the data subject does not need to use his right of access to know what data are processed and whether or not they are correct. In these situations, the data subject is not obligated to exercise his right of access, and wait for the controller to respond, before utilizing his other rights.

The right of access is also granted by Article 12(a) of the Data Protection Directive. However, a controller is obligated to provide more information under the GDPR.²² For example, he has to inform the data subject about the envisaged retention period or the criteria to determine that period. The additional information also relates to the other rights of the data subject. Under the Data Protection Directive, the controller had to inform the subject about the logic involved in any automatic processing of personal data. Pursuant to Article 15(1)(h) of the GDPR, this information has to be meaningful. Furthermore, it is supplemented by information about the significance and the envisaged consequences of such processing for the data subject. Finally, the controller has to inform the data subject about his other rights and the possibility to lodge a complaint with a supervisory authority pursuant to Article 15(1)(e) and (f). This information does not have to be provided under the Data Protection Directive.

The additional information allows a data subject to make a decision about the exercise of his rights based on concrete information about existing processing operations instead of an abstract privacy statement at the time of the collection of the data.²³ Specifically, the information about retention periods and automatic processing facilitates the exercise of the right to be forgotten and the right to obtain human intervention. Moreover, the additional obligations ensure that a data subject is again (section “Information and

communication”) made aware of the existence of his rights.

RIGHT TO RECTIFICATION AND COMPLETION

Pursuant to Article 16 of the GDPR, a data subject has the right to obtain from the controller the rectification of inaccurate personal data concerning him. He also has the right to complete the data if they are incomplete in the light of the purposes of the processing. Article 19 obligates the controller to communicate the rectification or completion²⁴ to the recipients to whom the personal data have been disclosed. This duty does not apply if the communication is impossible or would involve disproportionate effort. Finally, the data subject has a right to information about the recipients.²⁵ This allows him to make sure that these recipients also use the correct data.

The right to rectification is also granted by Article 12(b) and (c) of the Data Protection Directive. The right to completion is not mentioned explicitly. However, like the GDPR,²⁶ the directive treats the right to completion as a part of the right to rectification. Article 12(b) states that the right to rectification exists if the processing does not comply with the provisions of the Data Protection Directive, in particular because of the incomplete or inaccurate nature of the data. Naturally, incomplete data can be “rectified” by completing it. Furthermore, the principle of accuracy formulated in Article 6(d) imposes a general duty to make sure that the data are accurate and complete. For this reason, the limitation to situations in which a processing does not comply with the Data Protection Directive is also of little consequence.

RIGHT TO BE FORGOTTEN

Pursuant to Article 17 of the GDPR, a data subject has a right to obtain from the controller the erasure of personal data concerning him. If the controller has made the data public, Article 17(2) obligates him to take reasonable steps to inform other controllers of the request to erase the personal data. Furthermore, Article 19 of the GDPR imposes a duty on the controller to communicate the erasure to the recipients

to whom the personal data have been disclosed (see also section “Right to rectification and completion”). Article 17(1) lists the grounds that grant the right to erasure. The right does not apply if the processing is necessary for the purposes listed in paragraph 3.

Article 17 of the GDPR does not only state that a data subject has the right to be forgotten in the listed situations. It also states that the controller has an obligation to erase the data under the same conditions. This wording suggests that this duty can also apply if the data subject does not actively exercise his right. Other articles of the GDPR impose a similar obligation to erase personal data. Pursuant to the Articles 5(1)(c) and (e) and (2), 24 and 25, the controller is responsible for the compliance with the principles of data minimisation and storage limitation. In particular, he is obligated to establish the periods in which the personal data are stored and the criteria that determine this period.²⁷

This interpretation of Article 17 is tenable if the personal data have to be erased for compliance with a legal obligation to which the controller is subject (paragraph 1 under e) or if the data subject takes another action against the processing, in particular by withdrawing his consent (under b) or by objecting to the processing (under c). However, this interpretation is problematic in the other situations listed in paragraph 1. In many cases, an unlawful processing (under d) can also be mended without erasing the personal data (see below section “Right to restriction of processing”). The erasure is not preferable if the data subject does not object to the further lawful processing of his data. The mere fact that the personal data have been collected in relation to the offer of information society services to a child (under f) does not justify the deletion of the data. After all, Article 8(1) of the GDPR formulates criteria under which the processing of this data is permissible.

For these reasons, the interpretation that the right to be forgotten creates a general obligation to erase the personal data even when the data subject does not actively exercise his right should be rejected.²⁸ There is space between the *right* of the data subject to obtain erasure pursuant to Article 17 and the *obligation* of the controller to erase the personal data pursuant to other clauses of the GDPR. For example, it is possible that a controller has fixed storage periods that comply with Article 25(2), while an individual data subject still has the right to obtain erasure pursuant to Article

17(1)(a) because the personal data are no longer necessary in relation to the purposes for which they were collected or processed.

The right to be forgotten is also granted by Article 12(b) and (c) of the Data Protection Directive.²⁹ Under the directive, the right applies if the processing of the personal data does not comply with the provisions of the Data Protection Directive. The GDPR provides a more detailed description of the situations in which the right can be exercised. However, the scope remains largely the same. For example, if the controller has a legal obligation to erase the personal data (Article 17, paragraph 1 under e of the GDPR) or is no longer allowed to process it because the data subject withdraws his consent (under b) or successfully objects to the processing (under c), the further processing of the personal data, including the storage,³⁰ would not comply with the Data Protection Directive or the GDPR. Similarly, the processing of personal data that are no longer necessary in relation to the purposes for which they were collected or otherwise processed (under a) would violate the principles of purpose limitation and data minimisation and would thus be unlawful (under d).³¹ However, the Data Protection Directive does not grant a right to be forgotten for personal data that are collected in relation to the offer of information society services to a child (under f).³² By expanding the right to be forgotten to this ground, the GDPR slightly broadens the scope.

RIGHT TO RESTRICTION OF PROCESSING

Pursuant to Article 18 of the GDPR, a data subject has the right to obtain from the controller the restriction of the processing of his personal data. If the data subject exercises his right, the controller shall only process the data with the subject’s consent, for the establishment, exercise, or defence of legal claims, for the protection of the rights of another natural or legal person or for reasons of important public interest. Furthermore, the controller remains allowed to store the personal data. After all, the erasure of the personal data would also be a processing operation pursuant to Article 4(2) of the GDPR. Paragraph 3 obligates the controller to inform the data subject before lifting the restriction. Again, Article 19 of the GDPR imposes a duty on the controller to communicate the restriction

to the recipients to whom the personal data have been disclosed (see also section “Right to rectification and completion”)

Article 18(1) lists the grounds under which the right to the restriction of processing exists. First, the right can be a temporary solution when there is a conflict about the accuracy of the personal data (under a, section “Right to rectification and completion”) or about the exercise of the right to object (under d, section “Right to object”). Next, the right to restriction of processing can be an alternative for the erasure of the personal data if the data subject needs them in relation to a legal claim (under c) or opposes the erasure of unlawfully processed data for another reason (under b, see also section “Right to be forgotten”).

In addition to the rights to rectification and completion and to be forgotten, Article 12(b) and (c) of the Data Protection Directive also grants the right to “block” the data if the processing does not comply with the Data Protection Directive. The right to restriction of processing under the GDPR has a slightly broader scope. It is expanded to also apply during the period between the exercise of a right by the data subject and the response by the controller. Pursuant to Article 18(1)(a) and (d), it covers the periods that enable the controller to verify the accuracy of the personal data and to demonstrate legitimate grounds that override the objections of the data subject. Under the Data Protection Directive, the processing would only not comply with the provisions if it is actually established that the data are incorrect or incomplete or that the data subject has successfully objected to the processing. Furthermore, the GDPR clarifies the right by spelling out the consequences of the exercise of the right to restriction of processing. Finally, it explicitly states which processing operations remain allowed.

RIGHT TO DATA PORTABILITY

Pursuant to Article 15(3) of the GDPR, the data subject has the right to receive a copy of his personal data (section “Right of access”). The right to data portability expands this right in several ways.³³ First, Article 20(1) of the GDPR states that the data subject has a right to transmit the data to another controller. Paragraph 2 grants him the right to have the data transmitted directly from one controller to another.

This does not *a contrario* mean that a data subject cannot transmit the personal data when the right to data portability does not apply. The GDPR assumes that a data subject can assert control over “his” data. The fact that the information is legitimately processed by a controller does not change this.³⁴

Furthermore, Article 20 of the GDPR states that the data should be provided in a structured, commonly used and machine-readable format. “Structured” means that the personal data fit in a data model that can be used to define and interpret the data. For example, the provided information should allow a computer to understand that the text “Pieter Wolters” refers to the name of the data subject and that “P.Wolters@jur.ru.nl” is his email address. This structure allows the recipients to use the provided data in their own computer systems. The format should also be “commonly used”. However, this does not obligate the controller to use a specific format. For this reason, the right to data portability does not guarantee that the recipient can actually use the data. This is only possible if the computer systems of the controller and the recipient are interoperable.³⁵

The right to data portability strengthens the control by the data subject over his data (section “Introduction”). Instead of just influencing the processing by existing controllers, it also allows him to “transfer” his data to other “new” controllers.³⁶ For example, a data subject who wishes to switch from Facebook to another social network, or to use another social network in addition to Facebook, will not have to rebuild his entire profile.

Article 20 of the GDPR restricts the right to data portability in several ways. First, the right only applies to personal data that have been provided by the data subject to the controller. It does not cover data that have been created by the controller. However, the Article 29 Data Protection Working Party states that the right does not only apply to data that are actively and knowingly provided by the data subject. It also covers information that is obtained by observing the subject.³⁷

Furthermore, the right only exists if the lawfulness of the processing is based on the consent of the data subject or on the necessity for the performance of a contract to which the data subject is a party. It does not apply if the processing is based on one of the other grounds of Article 6(1) of the GDPR. For example, it does not apply if the processing is necessary for

compliance with a legal obligation or for the performance of a task carried out in the public interest.³⁸ Next, the right to data portability only exists if the processing is carried out by “automated means”. This concept is not defined in the GDPR. The Article 29 Data Protection Working Party states that most paper files are excluded.³⁹

Finally, Article 20(4) of the GDPR states that the right to data portability shall not adversely affect the rights and freedoms of others. Such an adverse effect could arise when the personal data also concern a third party. For example, the information that a data subject has received email from a third party, also means that the third party has sent this email. In principle, this “silent party data” is included in the right to data portability. The lawfulness of the processing of this data by the “new” controller can be based on the legitimate interest of the controller and the data subject (Article 6(1)(f) of the GDPR). After all, a data subject cannot effectively transfer his email if this information is not included. Of course, the new controller can only process the silent party data for the purpose of providing a service to the data subject. He cannot use the data to create a profile about the third party or to approach it with commercial offers. For this reason, the processing of silent party data does not adversely affect the rights and freedoms of the third party.⁴⁰

The right to data portability is new. It is not included in the Data Protection Directive. However, the importance of this right should not be overestimated. A data subject can also obtain a copy of his personal data by exercising his right of access. Although the controller has to communicate this information in an intelligible form, the Data Protection Directive does not obligate him to provide the data in a structured, commonly used and machine-readable format.

RIGHT TO OBJECT

Pursuant to Article 21 of the GDPR, the data subject has the right to object to a processing of his personal data. The criteria for this right depend on the processing that is objected to. First, paragraph 2 grants the data subject the right to object at any time to the processing of his data for direct marketing purposes. If he exercises this right, the controller is no longer allowed to process the data for these purposes pursuant to paragraph 3.

Next, paragraph 1 grants the data subject the right to object to the processing of his data which is based on Article 6(1)(e) or (f) of the GDPR. Contrary to an objection against the processing for direct marketing, the exercise of this right must be based on grounds relating to his particular situation. Furthermore, the controller will not always be obligated to stop the processing. He can continue if he can demonstrate “compelling legitimate grounds” for the processing that override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims (see also section “Right to restriction of processing”).

Under the criteria of paragraph 1, the successful exercise of the right to object depends on a comparison of interests. The interests, rights, and freedoms of the data subject that are affected by the processing must be weighed against the performance of the task carried out in the public interest or the exercise of official authority (Article 6, paragraph 1 under e) or the legitimate interests of the controller or a third party (under f) that is facilitated by the processing. This kind of comparison of interests is also incorporated in Article 6(1)(f). However, there will again (see section “Right to be forgotten”) be space between the lawfulness of the processing and the use of the right to object. It is possible that the processing of the personal data of a group of persons is allowed pursuant to Article 6(1)(f), but an individual data subject can still successfully object.⁴¹

A data subject cannot use his right to object if the processing is based on one of the other grounds of Article 6(1) of the GDPR. The right cannot be used against a processing that is necessary for compliance with a legal obligation (under c) or for the protection of vital interests (under d). Even if it could be used in these situations, the controller would almost certainly be able to demonstrate “compelling legitimate grounds” that override the interests of the data subject.⁴² Furthermore, a data subject can act against processing operations by not entering into or ending contracts that necessitate the processing (under b) or by withdrawing his consent (under a and Article 7, paragraph 3).

Finally, Article 21(6) grants the data subject the right to object to the processing of his personal data for scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR. Again, the objection must be based on grounds relating to his particular situation. If this criterium is met,

the controller cannot appeal to compelling legitimate grounds. However, he can continue to process the personal data if the processing is necessary for the performance of a task carried out for reasons of public interest. The GDPR does not clarify how this exception relates to Article 21(1). Paragraph 1 grants the right to object against a processing that is based on a task carried out in the public interest. However, paragraph 6 restricts this right if the data are processed for both a task of public interest and scientific or historical research purposes or statistical purposes. It does not require these grounds to override the interests, rights, and freedoms of the data subject.

The right to object is also granted by Article 14 of the Data Protection Directive. This article does not make an explicit exception for the situation that the controller demonstrates compelling legitimate grounds for the processing that override the interests of the data subject. However, it does require that the data subject bases his objection on *compelling legitimate* grounds relating to his particular situation. Furthermore, the controller is only obligated to stop processing the data if the objection is “justified”. Finally, Article 14 does not create a right to object to the processing for scientific or historical research purposes or statistical purposes.

RIGHT TO OBTAIN HUMAN INTERVENTION

Article 22(1) of the GDPR states that a data subject has the right not to be subject to a decision based solely⁴³ on automated processing or profiling⁴⁴ which produces legal effects concerning him or similarly significantly affects him. In reality, this “right” is a prohibition.⁴⁵ Paragraph 1 does not require any action by the data subject.

According to recital 71, Article 22(1) also applies to the automatic refusal of an online credit application or e-recruiting practices without any human intervention. Indeed, these kinds of decisions significantly affect the data subject. However, this does not mean that it is never allowed to use profiling to enter into (personalized) contracts.⁴⁶ Pursuant to paragraph 2, the prohibition does not apply if the decision is necessary for entering into, or the performance of, a contract between the data subject and the controller (under a), is authorized by national or European law

which also lays down suitable measures to safeguard the data subject’s rights, freedoms and legitimate interests (under b), or is based on the explicit consent⁴⁷ of the data subject (under c). Article 22(4) of the GDPR creates additional requirements for decisions that are based on the special categories of personal data referred to in Article 9. However, Article 9(2)(a) determines that these data can also be processed if the data subject has given explicit consent.

If the exception of Article 22(2)(a) or (c) applies, paragraph 3 obligates the controller to implement suitable measures to safeguard the data subject’s rights, freedoms, and legitimate interests. He must take steps to prevent mistakes and discriminating effects.⁴⁸ The data subject should at least have the right to obtain human intervention, to express his point of view and to contest the decision. If the data subject exercises these rights, the controller is obligated to make a new decision that is not solely based on automated processing.⁴⁹ Instead, the decision should involve a “meaningful” human element. The reviewer must have the authority and capability to change the decision.⁵⁰

Pursuant to the Articles 13(2)(f), 14(2)(g), and 15(1)(h) of the GDPR, the data subject has a right to meaningful information about the existence of automated decisionmaking, the logic involved and the significance and envisaged consequences of such processing for the data subject. Furthermore, recital 71 grants a right to an explanation of the reached decision. However, the controller has no obligation to precisely disclose how the utilized algorithm led to a particular decision in a specific case.⁵¹ Nonetheless, Article 15(1)(a) and (b) does grant the data subject the right to know what personal data are used for what purposes (see section ‘Right of access’). Through these safeguards, the right to obtain human intervention does not function as an absolute barrier against decisions based on automated processing, but as a tool to control and monitor these decisions.

The right to obtain human intervention is also granted by Article 15 of the Data Protection Directive. Compared to the directive, The GDPR demands stricter measures to protect the data subject. Article 15(2)(a) of the Data Protection Directive merely demands that the data subject is allowed to present his point of view. Furthermore, the Articles 10 and 11 of the Data Protection Directive do not impose a general duty to inform the data subject about the existence of and logic involved in the automatic

processing. Such an obligation exists only if the data subject actively exercises his right of access. Finally, the directive does not impose additional safeguards if the decision is based on the processing of special categories of personal data.

The Data Protection Directive does not contain an exception for decisions that are based on the explicit consent of the data subject. For this reason, the GDPR also leads to a weakening of the protection of data subjects. The regulation allows controllers to make decisions based solely on automated processing in additional situations.

MODALITIES IN RELATION TO THE EXERCISE OF THE RIGHTS OF THE DATA SUBJECT

The data subject can only benefit from his rights if the controller honours them in a manner that contributes to the protection of and control over his personal data. For example, a data subject is not aided by a right of access if he receives only a response after a long time has passed or if he cannot understand the provided information. For this reason, the articles that grant the rights also stipulate modalities in relation to the exercise of the rights and the performance of the corresponding obligations by the controller. Furthermore, Article 12 of the GDPR gives several general rules. According to recital 59, these rules aim to facilitate the exercise of the rights. They relate, in particular, to the communication with the data subject (section “Information and communication”), the facilitation of the exercise of the rights (section “Facilitation”), the time period in which the controller should honour the rights (section “Terms”), and the fees for the exercise of the rights (section “Fees”).

INFORMATION AND COMMUNICATION

Pursuant to the Articles 13(2)(b) and (f), 14(2)(c) and (g), and (3) and 21(4), the controller is obligated to provide information about the various rights of the data subject at the time of the collection of the data, after obtaining them from another source or at the time of the first communication with the data

subject. However, many data subjects will not read or benefit from this information at that time. After all, the personal data of a single person are processed by many controllers (section “The position of the data subject”). Furthermore, a data subject may only want to exercise his rights at a later time. For example, a data subject is more likely to use his right to be forgotten after not using an online service for an extended period than at the time of the first use of the service. Still, the fact that he is regularly made aware of his rights, may make the data subject aware that he can also exercise them at other times and against other controllers.

Under the GDPR, the controller is obligated to again provide this information if the data subject exercises his right of access (see section “Right of access”). In this situation, the data subject is already actively taking control over the processing of his personal data. He may be more inclined to exercise his other rights. Moreover, the data subject can make this decision based on more concrete information about existing processing operations.

Articles 10(c) and 11(1)(c) of the Data Protection Directive only obligate the controller to inform the data subject about the right of access and the right to rectification. Moreover, this duty only exists insofar as this information is necessary to guarantee fair processing in respect of the data subject. Next, except for information about the logic in the case of automated decisions, the controller is not obligated to again inform the data subject about his rights at the time of the exercise of his right of access.

Article 14(b) of the Data Protection Directive obligates *the member states* to take the necessary measures to ensure that data subjects are aware of the existence of the right to object against the processing of their personal data for purposes of direct marketing. In contrast to the other discussed provisions of the Data Protection Directive, Article 14(b) does not explicitly state that the *controller* should have an obligation. Naturally, a member state can fulfil its duty to inform the data subjects by forcing the controllers to provide the information.⁵² The directive does not contain an information duty in relation to the right to object to other processing operations.

Pursuant to Article 12(1) of the GDPR, the controller is obligated to communicate about the exercise of the rights of the data subject in a concise, transparent, intelligible, and easily accessible form,

using clear and plain language. This obligation allows a data subject to more easily monitor whether the controller adequately handles his requests. However, the controller is not required to make sure that every data subject is truly able to understand the provided information. Instead, Article 12 merely stipulates that he must take appropriate measures towards this goal.

The Data Protection Directive does not contain a general obligation to communicate clearly. Article 12(a) merely states that if the data subject exercises his right of access, the communication of the processed data should be in an intelligible form (sections “Right of access” and “Right to data portability”).

FACILITATION

Pursuant to Article 12(2) of the GDPR, a controller is obligated to facilitate the exercise of the rights of the data subject. According to recital 59, he must provide mechanisms that allow data subjects to exercise their rights more easily. Furthermore, the controller should facilitate electronic requests. For example, he could offer an online template on his Web site.⁵³ In any case, the controller cannot hide behind an unclear Web site and a hard to find email or postal address. The Data Protection Directive does not contain an obligation to facilitate the exercise of the rights of the data subject.

Article 12(2) of the GDPR strengthens the control by the data subjects. It forces the controller to actively enable the data subject to exercise their rights. However, the real effect of this obligation depends on its interpretation. After all, Article 12(2) does not prescribe any concrete measures.

TERMS

Pursuant to Article 12(3) of the GDPR, the controller must respond to a request concerning the exercise of the rights of the data subject without undue delay and in any event within 1 month of the receipt of the request. This period may be extended by 2 months if this is necessary due to the complexity and the number of the requests. Article 12(3) is foremost about the period within which the controller should *communicate* with the data subject. However,

the reaction should also provide information on the actions taken in response to the request. This suggests that the controller should also *perform* the obligations that correspond with the right within the provided term. With a few exceptions,⁵⁴ the GDPR does not explicitly stipulate the length of these terms. If the controller does not take action on the request of the data subject, he must inform the data subject without delay and at the latest within 1 month pursuant to Article 12(4). This response should give the reasons for not taking actions and inform the data subject about his rights to lodge a complaint with a supervisory authority and to seek a judicial remedy.⁵⁵

Article 12(3) of the GDPR is a clear improvement over the Data Protection Directive. Article 12 of the directive merely states that the right of access should be honoured without excessive delay. The Data Protection Directive does not give any guidance about the terms for the response to a request concerning the exercise of the other rights of the data subject.

FEES

Pursuant to Article 12(5) of the GDPR, a data subject can exercise his rights free of charge. A controller can only charge a reasonable fee or refuse to act if the requests of the data subject are manifestly unfounded or excessive, in particular because of their repetitive character. This starting point does not exist under the Data Protection Directive. Article 12(a) of the directive only stipulates that the data subject should be able to exercise his right of access without excessive expense. Pursuant to Case C-486/12, X [2013] ECLI:EU:C:2013:836, the controller cannot charge a fee that exceeds the cost of communicating such data. An objection to direct marketing is free of charge pursuant to Article 14(b) of the Data Protection Directive. The directive does not explicitly state whether a fee can be charged for the exercise of the other rights of the data subject.⁵⁶

Although the fees for the exercise of the right of access must be modest, they can still create a significant barrier to the exercise of the rights of the data subject. In practice, the right of access is a logical first step toward the exercise of the other rights (section “Right of access”). By allowing the controller to ask a fee for the exercise of the right of access, the other rights are also effectively locked behind this fee.

Furthermore, even assuming that the fee is negligible in comparison to the material or immaterial benefits of *ending or correcting* an unlawful processing, it may still provide a barrier to actively asserting *control*. Even if the fee is nominal, a data subject may not be inclined to use his right of access proactively in order to monitor the processing of his personal data. Instead, he will only exercise his rights if he knows or has a clear indication that his data are processed unlawfully. A data subject may not be able to determine this (section “The position of the data subject”). The right of access is aimed at facilitating this assessment. By making this right free of charge, the GDPR induces the data subject to more actively assert control over his data.

SYNTHESIS

The previous sections provide an overview of the rights of the data subject and the differences between the GDPR and the Data Protection Directive. The remainder of this article assesses the extent to which GDPR leads to a strengthening of the rights and control by the data subject. I will consecutively discuss the effects of the rights themselves (section “Scope and content”) and of the modalities in relation to their exercise (“Modalities”).

SCOPE AND CONTENT OF THE RIGHTS

The GDPR strengthens several rights. For example, it gives the data subject a right to additional information (section “Right of access”) and to have his data sent to another controller in a structured, commonly used, and machine-readable format (section “Right to data portability”). Furthermore, the GDPR grants additional safeguards in the case of automated processing (section “Right to obtain human intervention”). Finally, a data subject can exercise his rights in additional situations (sections “Right to be forgotten”, “Right to restriction of processing” and “Right to object”). Although these changes can be important in specific situations, they are relatively limited compared to the total scope of the rights under both the Data Protection Directive and the GDPR. It is unlikely that they lead to

a substantial strengthening of the control by the data subject.

Next, the GDPR clarifies and further develops the rights of the data subject.⁵⁷ For example, it more clearly defines the situations in which a data subject can use his right to be forgotten. Furthermore, the GDPR explicitly states that a data subject can also complete incomplete data (section “Right to rectification and completion”). Next, it clarifies the consequences of the exercise of the right to restriction of processing (section “Right to restriction of processing”). Finally, it provides more detailed rules in relation to the requirements for a successful objection to a processing that is based on Article 6(1)(e) or (f) of the GDPR. It clarifies that the successful exercise of this right can depend on a comparison of interests (section “Right to object”). These clarifications allow a data subject to more easily determine the scope and content of his rights. They lower the threshold to exercise them.

The more detailed text of the GDPR also clarifies the situations in which the rights of the data subject do not apply. For example, Article 17(3) lists several exceptions to the right to be forgotten that are not explicitly included in the Data Protection Directive. These new exceptions can weaken the position of the data subject. To illustrate, the prohibition of decisions that are solely based on automated processing does not apply under the GDPR if the processing is based on the explicit consent of the data subject (section “Right to obtain human intervention”).

MODALITIES

The Data Protection Directive hardly contains rules about the modalities for the exercise of the rights of the data subject. These matters are left to the national implementations. This means that the exact rules relating to the exercise of the rights of the data subject are different in each member state.⁵⁸ By including them in the GDPR, the regulation strengthens the position of the data subjects in several ways.

First, it allows a data subject to use the exact same rights with the same practical modalities in all situations in which the GDPR applies. This can lower the threshold to exercise the rights against controllers in other (European) countries.⁵⁹ The GDPR strengthens the rights of the data subject by harmonizing them.⁶⁰

Secondly, the GDPR provides and clarifies uniform modalities for the exercise of all the rights of the data subject. Again (see also section “Scope and content of the rights”), this allows a data subject to more easily understand them. It lowers the threshold to exercise the rights.

Finally, the content of the modalities also strengthens the position of the data subject. They ensure that a data subject is aware of his rights and understands them (section “Information and communication”) and is able to exercise them (section “Facilitation”) for free (section “Fees”). Although the maximum term of one or 3 months can be quite long (section “Terms”), it at least provides a clear enforceable limit.

The effect of the rights of the data subject and the modalities in relation to their exercise ultimately depends on the controller. A controller who does not adequately handle personal data may also not be inclined to communicate clearly, facilitate the exercise of the rights, or respond within 1 month.⁶¹ This could prevent a data subject from becoming aware of his rights or exercising them. This is a problematic result. The rights and control by the data subject are a tool. They are ultimately meant to strengthen the protection of personal data (section “Introduction”). Because the accessibility depends on the controller, the rights may not be practically available in the situations in which they are most needed.

The extent to which the rights strengthen the control by the data subject partly depends on the enforcement of the modalities in relation to the exercise of the rights. However, a data subject does not have a stand-alone interest in the application of these rules. They do not care about information about or the facilitation of the rights unless they are planning to exercise them. For this reason, the modalities are not likely to be enforced by individual data subjects. Instead, this will have to be done by supervisory authorities or non-governmental organisations.

CONCLUSION

In this article, I answer the following research questions: *What are the rights of the data subject under the GDPR? To what extent do these rights strengthen the control over the processing of his personal data?* The sections “Right of access” through “Right to obtain

human intervention” present an overview of the rights of the data subject and the differences between the GDPR and the Data Protection Directive. Although the GDPR does not significantly expand the rights, it does provide clarity about their legal effects and the exact criteria for their exercise (section “Scope and content of the rights”). Furthermore, the regulation gives more detailed rules in relation to the exercise of the rights and the performance of the corresponding obligations by the controller (section “Modalities in relation to the exercise of the rights of the data subject”). These modalities lower the threshold for the data subject. They make it easier for him to exercise his rights by clarifying the process and removing barriers (section “Modalities”). For these reasons, the GDPR considerably strengthens the *rights* of the data subject.

At the same time, this enhancement only marginally alleviates his disadvantaged position. The personal data of a single data subject will still be processed by many controllers and in many different ways. The GDPR does not grant him any tools to practically maintain an overview of these controllers and processing operations. For example, the option to erase personal data that were collected when he was a child (section “Right to be forgotten”) does not enable the data subject to realize who has his data after he becomes an adult. Similarly, the exact consequences of individual processing operations will remain hard to establish. In many situations, the GDPR will not in itself create a stimulus to exercise the rights of the data subject (section “the position of the data subject”).

For these reasons, the strengthening of the *control* by the data subject is limited. The GDPR allows a data subject to more easily exercise his rights if there is a clear indication that his data are not adequately protected. The rights of the data subject, however, do not induce or permit him to proactively and substantially assert control over the processing of his personal data.⁶² As long as the data subject remains in a disadvantaged position, his role will continue to be correcting instead of controlling.

NOTES

1. European Parliament and Council Regulation 2016/679/EU of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

- About these concepts, see GDPR, art 4(1), (7), (8). About the obligations, see, for example, Viviane Reding, 'The European data protection framework for the twenty-first century' (2012) 2 IDPL 119, 126–127; Yann Padova, 'What the European Draft Regulation on Personal Data is going to change for companies' (2014) 4 IDPL 39, 45–49; Bart van der Sloot, 'Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation' (2014) 4 IDPL 307, 311–314; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 CLSR 179, 190–193.
2. European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31; GDPR, Arts 94, 99.
 3. See, for example, GDPR, recitals 2, 7, 9, 10, 11, 13; Reding (n 1) 121; Van der Sloot (n 1) 317; Jan Philipp Albrecht, 'How the GDPR Will Change the World' (2016) 2 EDPL 287, 288; P.T.J. Wolters, 'The security of personal data under the GDPR: a harmonized duty or a shared responsibility?' (2017) 7 IDPL 165, 165.
 4. Van der Sloot, *supra*, n 1, 317.
 5. About these concepts, see GDPR, Art 4(1), (2).
 6. Section 'The position of the data subject'; GDPR, recitals 7, 11, 63, Reding (n 1) 124–125; Peter Blume, 'The myths pertaining to the proposed General Data Protection Regulation' (2014) 4 IDPL 269, 270; Padova, *supra* n.1, 40–43; Van der Sloot, *supra*, n.1, 314–316; Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed 3, 6–20; De Hert and Papakonstantinou, *supra* n.1, 188–190; Veale, Binns and Ausloos, *supra* n.4, 3; Jef Ausloos and Pierre Dewitte, 'Shattering one-way mirrors – data subject access rights in practice' (2018) 8 IDPL 4, 7–8, 22; 'Rights for citizens', *ec.europa.eu* (2 march 2018). About the importance of the control by the data subjects, see also GDPR, recitals 75, 78, 85. About the relation between these rights and control, see also Anneliese Roos, 'Core Principles of Data Protection Law (2006) 39 Comp. Int'l L.J. S. Afr. 102, 119.
 7. Cf. GDPR, Arts 13, 25.
 8. Dan Svantesson, 'Enter the quagmire – the complicated relationship between data protection law and consumer protection law' (2018) 34 CLSR 25, 28.
 9. Cf. GDPR, art 2(2)(c). The GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.
 10. See also Van der Sloot, *supra* n.1, 322–324.
 11. For example, the personal data of a person might be processed by his employer, his municipal authority, the school(s) of his children, his insurance company, web shops from which he has made a purchase, his telephone company, the providers of services such as Spotify and Netflix, online search engines, social media, ad-trackers, and other websites that use cookies.
 12. Bert-Jaap Koops, 'The trouble with European data protection law' (2014) 4 IDPL 250, 252; Van der Sloot, *supra* n.1, 323; Lazaro and Le Métayer, *supra* n.6, 10, 23–24; Tom Symons and Theo Bass, *Me, my data and I: The future of the personal data economy* (2017), 20.
 13. Van der Sloot, *supra* n.1, 323; Lazaro and Le Métayer, *supra* n.6) 10–11; Ausloos and Dewitte, *supra* n.6, 22.
 14. European Commission, *Data Protection* (Special Eurobarometer 431, 2015) 6–14.
 15. Reding, *supra* n.1, 125; Blume, *supra* n.6, 270; Koops, *supra* n.12, 252; Van der Sloot, *supra* n.1, 322; Lazaro and Le Métayer, *supra* n.6, 30131; Ausloos and Dewitte, *supra* n.6, 4–5.
 16. Koops, *supra* n.12, 252; Lazaro and Le Métayer, *supra* n.6, 23; Ausloos and Dewitte, *supra* n.6, 21. See section 'Right of access'.
 17. See also Koops, *supra* n.12, 251–252; section 'Right to data portability'.
 18. Van der Sloot, *supra* n.1, 322–324; Lazaro and Le Métayer, *supra* n.6, 12–14, 27. The rights can also be exercised collectively. Ausloos and Dewitte, *supra* n.6, 22–23.
 19. See also sections 'Right to rectification and completion', 'Right to be forgotten', 'Right to obtain human intervention'.
 20. In the context of the Data Protection Directive, see Case C-141/12 and 372/12, Y.S. [2014] ECLI:EU:C:2014:2081. See also Case C-553/07, *Rotterdam/Rijkeboer* [2009] ECLI:EU:C:2009:293; Ausloos and Dewitte, *supra* n.6, 7.
 21. Cf. the Dutch implementation of the Data Protection Directive: *Wet Bescherming Persoonsgegevens*, Art 36 (*Stb.* 2000, 302, last amended in *Stb.* 2017, 317, rescinded in *Stb.* 2018, 144), in which the rights of rectification, the right to be forgotten and the right to restriction are limited in this manner.
 22. Cf. GDPR, Art 15(1) and Data Protection Directive, Art 12(a). See also Ausloos and Dewitte, *supra* n.6, 18–19.
 23. See also Ausloos and Dewitte, *supra* n.6, 22.
 24. The GDPR treats the right to completion as a part of the right of rectification. It is not named in Article 19 or the other recitals or articles about the rights of the data subject. GDPR, Arts 13(2)(b), 14(2)(c), 15(1)(e), and 58(2)(g), recitals 39, 59, 65, 73, and 156. Cf. GDPR, Arts 12(2) (data subject rights under Articles 15 to 22), 23(1) (obligations and rights provided for in Articles 12 to 22), in which none of the rights are named.
 25. This right is also granted by the right of access. Pursuant to Article 15(1)(c) of the GDPR, a controller is obligated to provide information about the recipients or categories of recipients to whom the personal data have been or will be disclosed.
 26. See also *supra* n.24.
 27. For example, GDPR, Arts 13(2)(a), 14(2)(a), 15(1)(d), 25(2), 30(1)(f), 47(2)(d), recital 39.
 28. Cf. GDPR, recital 65.
 29. See also Case C-131/12, *Google Spain* [2014] ECLI:EU:C:2014:317; Reding, *supra* n.1, 125; Blume, *supra* n.6, 270.
 30. GDPR, Art 4(2); Data Protection Directive, Art 2(b). See also section 'Right to restriction of processing'.
 31. GDPR, Art 5(1)(b), (c); Data Protection Directive, Art 6(1)(b)(c).
 32. See also GDPR, recital 65; Reding, *supra* n.1, 125; Van der Sloot, *supra* n.1, 315.
 33. Reding, *supra* n.1, 125; Paul De Hert and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 CLSR 193, 201.
 34. Section 'Introduction'; Padova, *supra* n.1, 41–42.
 35. GDPR, recital 68; Article 29 Data Protection Working Party, *Guidelines on the right to data portability* (16/EN WP 242 rev.01, 2017) 17–18; De Hert and others, *supra* n.33, 197, 200–201. Cf. GDPR, Art 20(2) (where technically feasible).
 36. De Hert and Papakonstantinou, *supra* n.1, 189; Article 29 Data Protection Working Party, *Data portability*, *supra* n.35, 4–5; De Hert and others, *supra* n.33, 195, 198, 201.
 37. Article 29 Data Protection Working Party, *Data portability*, *supra* n.35, 9–10; De Hert and others, *supra* n.33, 199–200. For example, the registration of a heartbeat, the use of a Web site or a search history. The right does not cover an assessment score or the analysis of the health of the data subject that is based on the observed heartbeat.
 38. GDPR, Art 6(1)(c), (e), recital 68; Article 29 Data Protection Working Party, *Data portability*, *supra* n.35, 8.
 39. Article 29 Data Protection Working Party, *Data portability*, *supra* n.35, 9.

40. Article 29 Data Protection Working Party, *Data portability*, *supra* n.35, 11–12. In the context of the right of access, cf GDPR, Art 15(4).
41. See in the context of the Dutch implementation of the Data Protection Directive the Explanatory Notes to the *Wet Bescherming Persoonsgegevens*, *supra* n.21. *Kamerstukken II 1997-98*, 25892, 3, 163 (MvT).
42. However, the data subject could demand the restriction until such interests are demonstrated. Section “Right to restriction of processing.”
43. As a starting point, the article does not apply if a person makes a decision based on the automatic processing of personal data. Mireille Hildebrandt, ‘The Dawn of a Critical Transparency Right for the Profiling Era’, in Jacques Bus and others (eds), *Digital Enlightenment Yearbook 2012* (IOS Press 2012) 51; Sandra Wachter, Brent Mittelstadt and Luciano Floridi, ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation’ (2017) 7 IDPL 76, 88-89, 92; Andrew D. Selbst and Julia Powles, ‘Meaningful information and the right to explanation’ (2017) 7 IDPL 233, 235. Cf., *supra* n.50.
44. About this concept, see GDPR, Art 4(4); Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (17/EN WP 251rev.01, 2018) 6–7.
45. Hildebrandt, *supra* n.43, 50; Wachter, Mittelstadt and Floridi, *supra* n.43, 94–95; Article 29 Data Protection Working Party, *Automated individual decision-making*, *supra* n. 44, 19–20, 34–35.
46. Cf. Gianclaudio Malgieri and Giovanni Comandé, ‘Why a right to legibility of automated decision-making exists in the general data protection regulation’ (2017) 7 IDPL 243, 253-254; Article 29 Data Protection Working Party, *Automated individual decision-making*, *supra* n.44, 21–22.
47. About this concept, see Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679* (17/EN WP259, 2017) 18–19.
48. GDPR, recital 71. See also Article 29 Data Protection Working Party, *Automated individual decision-making*, *supra* n.44, 32 for various good practice recommendations.
49. Article 29 Data Protection Working Party, *Automated individual decision-making*, *supra* n.44, 35.
50. Malgieri and Comandé, *supra* n.46, 251–252; Article 29 Data Protection Working Party, *Automated individual decision-making*, *supra* n.44, 21 and 27.
51. Wachter, Mittelstadt and Floridi, *supra* n.43, 79–90; Article 29 Data Protection Working Party, *Automated individual decision-making*, *supra* n.44, 25, 27. Cf. Selbst and Powles, *supra* n.43, 235–241; Malgieri and Comandé, *supra* n.46, 255–257.
52. For example, *Wet Bescherming Persoonsgegevens*, *supra* n.21, Art 41(4); *Bundesdatenschutzgesetz*, § 28(4) (*Bundesgesetzblatt* 2003, Teil I, 66, last amended in *Bundesgesetzblatt* 2009, Teil I, 2814, rescinded in *Bundesgesetzblatt* 2017, Teil I, 2097).
53. See also Xavier Duncan L’Hoiry & Clive Norris, ‘The honest data protection officer’s guide to enable citizens to exercise their subject access rights: lessons from a ten-country European study’ (2015) 5 IDPL 190, 197; Ausloos and Dewitte, *supra* n.6, 23.
54. GDPR, Arts 16, 17 (both “without undue delay”).
55. GDPR, Arts 77, 79.
56. Since the Data Protection Directive only states that the right to object to direct marketing must be free of charge, one could *contrario* conclude that a fee can be asked for the exercise of the other rights. Cf. *Wet Bescherming Persoonsgegevens*, *supra* n.21, Art 40(3) (a controller may ask a fee if the data subject objects to the processing of his personal data for other purposes than direct marketing).
57. De Hert and Papakonstantinou, *supra* n.1, 188. The European Commission had the authority to elaborate on the various rights under the original proposal. This power has been removed in the enacted regulation. De Hert and Papakonstantinou, *supra* n.1, 186 and 189. The European Commission remains empowered to adopt rules in relation to the use of standardized icons to provide information. GDPR, Art 12(8).
58. De Hert and Papakonstantinou, *supra* n.1, 188; Ausloos and Dewitte, *supra* n.6, 18.
59. About the territorial scope of the national implementations, see Data Protection Directive, Art 4.
60. About the effect of harmonization on the protection of the data subjects, see GDPR, recitals 2, 7, 9, 10, 13; Reding, *supra* n.1, 121, 127; Van der Sloot, *supra* n.1, 316–320; Albrecht, *supra* n.3, 288; Simon Davies, ‘The data protection regulation: a triumph of pragmatism over principle?’ (2016) 2 EDPL 290, 293–294; De Hert and Papakonstantinou, *supra* n.1, 182; Wolters, *supra* n.1, 165.
61. For empirical studies about the exercise of the right of access, see L’Hoiry, *supra* n.53, 194–195; René L.P. Mahieu, Hadi Asghari and Michel van Eeten, ‘Collectively Exercising the Right of Access: Individual Effort, Societal Effect’ (12th GigaNet Annual Symposium, Geneva, December 2017); Ausloos and Dewitte, *supra* n.6, 10–18. Cf. Veale, Binns and Ausloos, *supra* n.4, 17–18 (the rights of the data subject can also be limited by other obligations).
62. See also Blume, *supra* n.6, 270; Koops, *supra* n.12, 252–253.

Copyright of Journal of Internet Law is the property of Aspen Publishers Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.