Data Processing Based on Legitimate Interests
Discussion Draft v5 – 29 December 2016

Following the precedent established by the 1996 EU Data Protection Directive, the EU General Data Protection Regulation (GDPR) provides that companies may justify processing activities based on the concept of their "legitimate interests." While the phrase "legitimate interest" is not explicitly defined, a solid understanding of this concept is critical to implementing GDPR compliance programs. Controllers must be able to engage in beneficial processing activities, while respecting the interests, rights and freedoms of the individual data subjects and other stakeholders.

This paper explores the concept of "legitimate interest" under the GDPR. It is meant to establish a common standard regarding the types of processing activities that should be reasonably expected by all stakeholders and therefore considered "legitimate" under the GDPR, as well as establishing a framework to assess various processing activities in a way that balances the controller's interests with societal interests and the interests, rights and freedoms of data subjects, using objective criteria.

A. GDPR Background

Companies subject to the EU General Data Protection Regulation (GDPR) may justify processing activities based on the concept of their "legitimate interests" per Article 6:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Although the phrase "legitimate interests" is not a defined term in the GDPR, this concept permeates the Regulation. Recital 47 states:

> The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of

> the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

Additionally, the controllers' legitimate interests in many cases appears to overlap with other legal bases for processing in Article 6. For example, Recital 49 of the GDPR acknowledges that controllers have a legitimate interest in processing needed to ensure security of networks and information systems, but this processing can also be justified as a being a task carried out in the public interest. Similarly, processing data for public health purposes might be done both as a legitimate interest of the controller and because it is necessary to protect the vital interests of the data subject.

B. GDPR Statements regarding Processing Activities Justified by Legitimate Interests

From the GDPR's guidance, we understand that the following types of processing activities may be justified on the basis of legitimate interests:

1. Processing of customer or client data, including for direct marketing (Recital 47)

- [W]here there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. [Provided that] the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

- The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

2. Processing of data among members of a corporate family or group of undertakings for internal administrative purposes (Recital 48)

- Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

3. **Processing of data to the extent strictly necessary for network and information security (Recital 49)**

   - The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

4. **Certain *ad hoc* data transfers (Recital 113)**

   Transfers which can be qualified as not repetitive and that only concern a limited number of data subjects, could also be possible for the purposes of the compelling legitimate interests pursued by the controller, when those interests are not overridden by the interests or rights and freedoms of the data subject and when the controller has assessed all the circumstances surrounding the data transfer. The controller should give particular consideration to the nature of the personal data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and should provide suitable safeguards to protect fundamental rights and freedoms of natural persons with regard to the processing of their personal data. Such transfers should be possible only in residual cases where none of the other grounds for transfer are applicable. For scientific or historical research purposes or statistical purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. The controller should inform the supervisory authority and the data subject about the transfer.

C. Assessing and Documenting Legitimate Interests

It is important to note that merely having a legitimate interest is not sufficient to justify the processing activities; the legitimate interest must not itself by outweighed by the rights and freedoms of the data subject. Controllers must consider if the data subject has a right to object to the processing, as discussed in Recital 69:

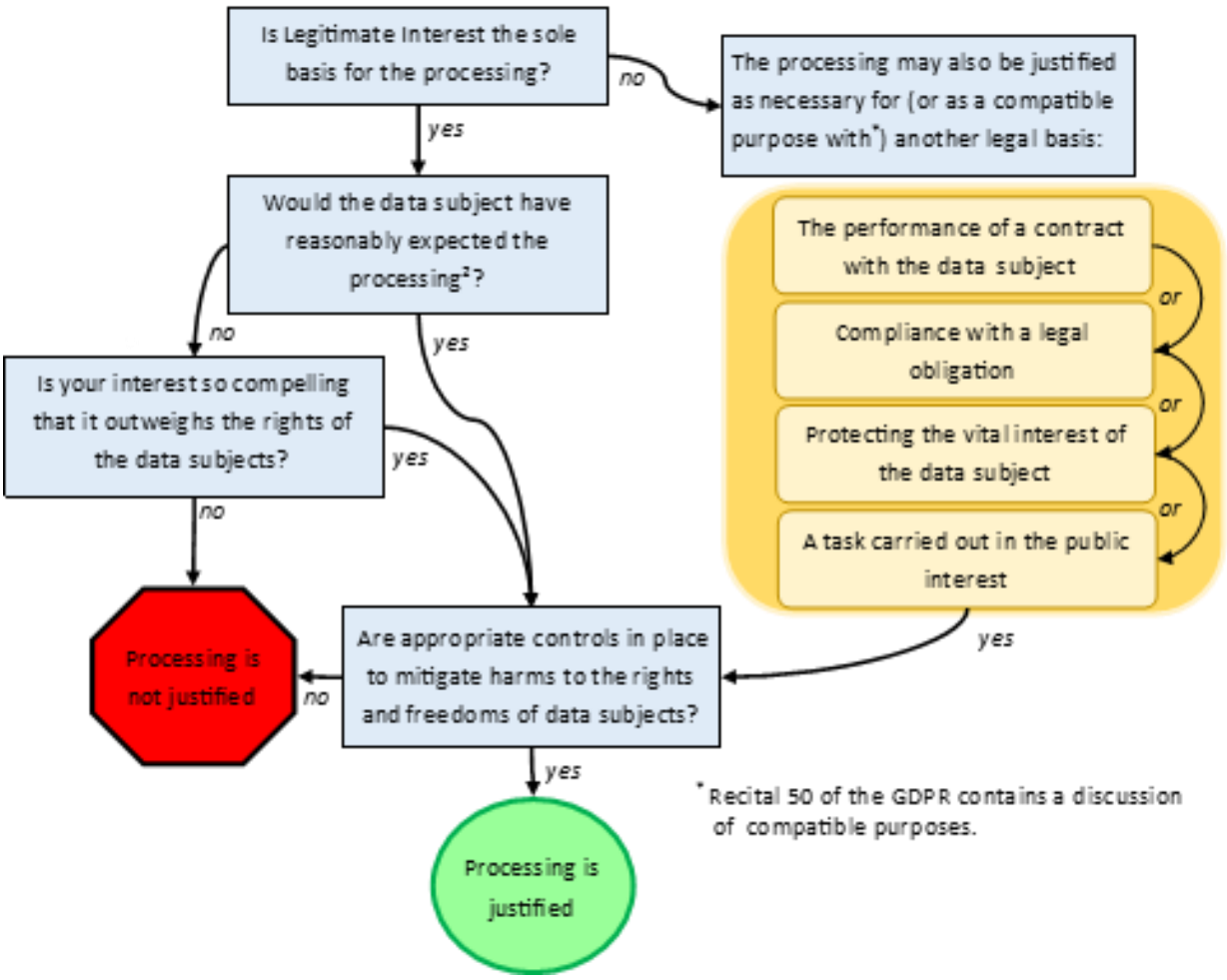
> Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

> authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.

Additionally, as is clear from Recital 47, prior to relying on a legitimate interest as a basis for processing, the controller must undertake an assessment to determine (1) whether the data subject would reasonably expect the processing (given the context of the collection of the data), and (2) whether the legitimate interest is overridden by the rights of the data subject. The implication from the guidance is that, should the processing not be reasonably expected, the rights and freedoms of the data subject may well prevail. ("The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.")

Taking all the factors presented in the GDPR into account, we can depict the assessment process as a flowchart that allows a controller to determine if processing based on legitimate interest is justified:

Can a Processing Activity Be Justified on the Basis of a Legitimate Interest?



D. Examples of Reasonably-Expected Processing Activities

As noted above, controllers that want to process personal data based on their legitimate interests should be able to demonstrate that the data subjects reasonably expected such processing to occur. The following matrix has been prepared to assist controllers, data subjects and supervisory authorities with determining what types of processing might be reasonable to expect. For simplicity, we can group these processing activities into five categories that generally reflect the strength of the company's interest, namely processing needed for:

1. **Protecting Individuals, Organizations or the Public**
   a. Public Health & Safety
   b. Security of Networks and Information Systems
   c. Fraud Detection, Prevention and Remediation
   d. Security Incident (Data Breach) Response
   e. Compliance with Local Laws And Regulatory Requirements

2. **Compliance with Laws and Regulatory Requirements from Other Jurisdictions**

3. **Standard Business Management, Internal Administrative Purposes and other functions that are directly related to the entity's relationship with the data subject**

4. **Relationship Management, Business Intelligence, and other functions that are indirectly related to the relationship with the data subject**

5. **First Party marketing, and other functions related to establishing or expanding the relationship with the data subject**

In each of these categories, we articulate in Annex 1 below some examples of the types of processing activities that are likely to occur for these purposes.[1] In assessing legitimate interest, these types of processing activities should be deemed "reasonably expected."

E. Balancing Legitimate Interests with Fundamental Rights and Freedoms

As noted above, merely having a legitimate interest is not sufficient to justify the processing activities; the legitimate interest must not itself by outweighed by the rights and freedoms of the data subject.

It is therefore necessary to consider how each of the categories of legitimate interests set forth above should be weighed or balanced against individual rights and freedoms. Clearly some types of processing activities, such as processing necessary to protect public health, are very compelling. In other instances, companies may have a legitimate interest in processing personal data, such as for direct marketing, but this interest would not necessarily outweigh an individual's right to object to the processing.

To support this balancing test, we must consider three distinct entities with interests, rights and freedoms: the data subject him or herself, the data controller, and other individuals whose interests

[1] It is, of course, impossible to offer a full list of legitimate processing activities as these will vary by industry and the nature of the relationship (consumer, customer, supplier, business partner, employee etc.

may be affected by the decision to process (or not) the data.[2] The following questions help establish the various interests, rights and freedoms that may be affected:

The Data Subject

- Does the processing benefit me? If so, by how much?
- Does the processing threaten my rights and freedoms? If so, by how much?
- Are there steps I can take to mitigate risk? If so, by how much?

The Controller

- Is the processing necessary to protect the rights and freedoms of others? If so, by how much?
- Does the processing benefit me? If so, by how much?
- Are there other legal bases for the processing?
- What steps can I take to mitigate risk?

Other Individuals (directly or via a societal interest)

- Does the processing benefit third parties or civil society? If so, by how much?
- Does the processing threaten third parties or civil society? If so, by how much?
- Can the threats be mitigated? If so, by how much?

From these questions, we can develop a set of case studies around the various categories of reasonably expected processing activities. These case studies are presented in the next section. In each case, the assessment considers the interests of all three entities: (1) data subject, (2) controller, and (3) other individuals.[3] It also considers the steps that the entities can take to mitigate risk.

In conducting any legitimate interest assessment, it is important to consider both the full range of interests as well as the full range of possible risks, including tangible risk (such as threats to physical well-being or potential for fraud), intangible risks (such as anxiety or embarrassment) and abstract risks (such as social stratification and threats to democracy).[4] Similarly, risk mitigation strategies should be considered broadly. Risks may be mitigated using technological controls as well as by policies and contracts. Risks may also be mitigated by program design changes, such as reducing identifiers, using a smaller pool of data for tests/proof of concept programs, and/or establishing controls to evaluate

[2] For example, a data subject might object to having her health data processed for research purposes, but other individuals with the same condition may have a compelling interest in having the research conducted. There is also a societal interest in medical research.

[3] The Article 29 Working Party's "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC" establishes a similar balancing test. As with the WP29 approach, this balancing test should not be viewed as an "open door to legitimize any data processing" but should rather provide a framework for considering the full spectrum of rights, including the public interest, risks, and risk mitigations.

[4] For a discussion of privacy risk and benefits, please see "Benefit-Risk Analysis for Big Data Projects" Future of Privacy Forum September 2014 (https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf) which defines the spectrum of privacy risks ranging from tangible risk (threats to physical well-being, financial loss, damage to livelihood, administrative inconvenience, security breach and confidentiality breach), intangible risks (reputational damage, creepy inferences, anxiety /embarrassment, unfair discrimination, exclusion and isolation)to abstract risk (panoptic surveillance, social stratification, filter bubbles, paranoia and loss of trust, chilling effect and threats to democracy).

inferences for intangible risks (such as creepiness). Controller adoption of data protection/privacy impact assessment programs (PIAs/DPIAs), together with Privacy by Design/Default methodologies should enable stakeholders to have confidence that the balancing tests used are effective and appropriate.

F. Use Cases Illustrating the Assessment of Legitimate Interest

The following use cases illustrate how the balancing test might be applied for certain types of processing activities in each category to verify that the interests are balanced and risks appropriately mitigated.

1. Sample Assessment of Processing to Protect Individuals, Organization and the Public

Sample Processing Activity: *Acme, a financial institution, verifies a consumer's identification document prior to completing a financial transaction. The Acme employee compares the photo and information on the document to that of the customer. The employee also uses an automated service to verify the authenticity and validity of the ID document presented.*

Consideration of Interests:

Controller	***Data Subject***	***Other Individuals, Society***
Acme has a compelling need to process data for fraud prevention both to mitigate individual and public harm and to protect itself from loss. Acme desires fast and reliable fraud detection processes, ideally that limit the amount of personal data (especially sensitive data) that must be collected and processed before a transaction can be approved.	Data subjects have a compelling need for Acme to process data for fraud prevention, as fraud is detrimental to them. Even if the data subject is not directly impacted by identity theft, company losses may result in an increase in the price of services. Data subjects also have an interest in having their identities verified quickly and accurately, using processes that require the minimum amount of data.	Other individuals have a compelling need for companies to prevent fraudulent transactions that are costly to the economic system.

Risk Mitigation: Risks are managed by Acme's application of the purpose limitation principles and technological controls. For example, the automated checking can be set to return a "pass" or "additional review required" value. For IDs that are verified, Acme does not store additional data. For ID that are not verified automatically, Acme conducts additional validation, using encryption and access controls to safeguard the information being processed.

Conclusion: Acme's compelling interest in preventing fraud is shared by data subjects and society. Acme's interest is efficiency and data minimization also justify the processing. Any residual risks (inherent risk minus mitigation) to the rights and freedoms of data subjects are overridden by the needed for anti-fraud processing to occur.

2. Sample Assessment of Processing for Compliance with Laws of Another Jurisdiction

Sample Processing Activity: *Beta, a US-based multi-national establishes a global program to comply with the U.S. Foreign Corrupt Practices Act[5] (FCPA). Beta's FCPA program processes personal information (including criminal records and allegations) pertaining to individuals and entities to verify that corrupt payments are not being made to influence foreign officials, directly or via an intermediary.*

Consideration of Interests:

Controller	***Data Subject***	***Other Individuals, Society***
Beta has a legitimate interest in operating globally. As a US company, Beta must also comply with applicable US laws. The FCPA prohibits US companies from making inappropriate payments to foreign government officials directly or via intermediaries. Failure to company with FCPA carries criminal and civil liability. Beta has a compelling interest in being able to demonstrate its compliance with FCPA. Beta also has a specific interest in ensuring that its business dealings do not involve any unlawful or corrupt payments to foreign government officials.	Data subjects, both foreign officials themselves and intermediaries involved in procuring business, have an interest in supporting company FCPA compliance, as this provides the basis for US companies to engage in commercial relationships in their countries. On the other hand, foreign officials in countries where payments for influence are expected (and not illegal) may be disadvantaged by the FCPA. However, this effect results from the law itself, not from any company's compliance program.	The FCPA was enacted to restore confidence in the integrity of American businesses. There is a strong societal interest in reducing public corruption globally. This interest is reflected in the extraterritoriality of the law. *Note that many countries have laws like the FCPA, and the OECD recommends specific organizational controls to prevent and detect foreign bribery.*

Risk Mitigation: Beta has an extensive training program for its employees regarding FCPA, and this program educates employees about the data processing needed to verify compliance. Processing risks are managed by Beta's application of the purpose limitation principles. While Beta's FCPA compliance program collects sensitive personal data pertaining to its employees, officials, relatives and business partners of officials and company intermediaries, the personal data is only be processed by Beta as needed to demonstrate FCPA compliance. Strong security controls, including encryption and access controls, protect personal data that the company needs to retain or archive for compliance purposes.

Conclusion: The societal interest in reducing corruption outweighs the costs to controllers and the risk to data subjects. Beta is taking steps to minimize risk associated with the processing, and any residual risks to the rights and freedoms of data subjects are overridden by the compelling interest of Beta to comply with this law.

[5] To learn more about the FCPA, please see https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

3. Sample Assessment of Processing for Standard Business Management Purposes

Sample Processing Activity: *Gamma, a company offering products for sale on its website requires online customers to establish an account by providing an email address and setting a username and password. This account information is required in addition to the information strictly need to process the transaction (name, mailing address and payment details). Individuals may login to their accounts to check order status and may use the account for additional orders or customer service purposes. Transactional communications (such as the order confirmation and shipping notices) are sent to the individual via email. If the person consents, Gamma may also send marketing information via email.*

Consideration of Interests:

Controller	***Data Subject***	***Other Individuals, Society***
Gamma has a clear interest in offering its products to consumers online. It also has a legitimate interest in collecting extra data elements as needed to facilitate the online relationship, ensure that it can communicate with the data subject and provide an appropriate mechanism for allowing the data subject to receive general information about the order electronically.	Data subjects have an interest in not being required to provide unnecessary or excessive elements of personal data. However, data subjects also have an interest in being able to efficiently and effectively engage in online shopping transactions. Gamma's collection of email address facilitates the online relationship in a reasonably unintrusive manner.	There is a societal interest in facilitating corporate transactions. Additionally, company shareholders, customers and employees have a general interest in the successful outcomes of mergers and acquisitions.

Risk Mitigation: Individuals who do not want to interact with Gamma via their online accounts can receive customer service through traditional (in-store or phone) channels. Unless the data subject consents to receive marketing communications, the email address will only be used to send communications about the individual's orders. Gamma may close accounts and delete personal data if the account is inactive for a defined period of time or if the consumer requests that the account be deactivated.

Conclusion: While Gamma is collecting personal data that are not strictly necessary, the risks associated with this activity are low and the process provides consumers with the benefits of a more efficient online shopping experience. Some data subjects may refrain from shopping with Gamma because of the requirements to provide an email and create an account, but these requirements are not unreasonable, and Gamma's legitimate interest justifies the processing.

Another example:

Sample Processing Activity: *Zeta, a company in the retail sector, is completing its acquisition of another retailer, Rho. To facilitate the integration, Zeta will process personal data pertaining to Rho's customers. This data will be used initially to determine which consumers are shared, and then to communicate information about the acquisition to all of Rho's customers. The data will also be used to enable Zeta to provide ongoing support to the Rho customers.*

Consideration of Interests:		
Controllers	***Data Subject***	***Other Individuals, Society***
Both companies have a legitimate interest in managing the integration of their operations in an appropriate and efficient manner. Zeta also needs to understand the consolidated customer base and to provide information to the customers regarding the new arrangement. Zeta will assume Rho's obligations to fulfill open opens, provide customer support and warranty support to the customers post-closing. It must process Rho customer data for these activities. Zeta also has a specific interest in developing strong relationships with Rho's customers, especially those individuals who are not currently doing business with it.	Rho's customers have an interest in controlling the use of their data by companies. In this case, while the consumers chose to do business with Rho, they did not choose to do business with Zeta. However, they also have an interest in having their commercial relationships handled efficiently, including having seamless order processing and customer service.	There is a societal interest in facilitating corporate transactions. Additionally, company shareholders, customers and employees have a general interest in the successful outcomes of mergers and acquisitions.
Risk Mitigation: As part of the acquisition due diligence, Zeta must evaluate Rho's privacy statements. If there are any material differences between the promises made by Rho and Zeta's practices, Zeta will handle the Rho customer information in accordance with Rho's privacy statement. Additionally, as part of the communications sent to the consumers, Zeta will provide the consumers with information about its privacy program, noting the differences (if any) and informing them about how to exercise their privacy rights. Should individuals object to Zeta's processing of their data, Zeta will take measures to close their accounts and only retain data needed to fulfill contractual obligations and for compliance.		
Conclusion: Zeta and Rho have a legitimate interest in sharing Rho's customer data as needed to complete their merger. The data subjects have the right to not have their data processed in ways that are incompatible with the privacy promises made by Rho. As long as Rho respects those promises and processes the data as needed for the integration, the legitimate interests of the companies will outweigh the rights of the individuals.		

4. Sample Assessment of Processing for Relationship Management Purposes

Sample Processing Activity: *Zeta offers its customers the opportunity to enroll in its "preferred customer" shopper program, which enables the customers to earn points toward free products based on their purchases. Zeta sends preferred customers email and direct mail promotional offers, including coupons and invitations to special events. As part of the first communication announcing its acquisition of Rho, Zeta plans to send a direct mail piece to those Rho customers who are not members of Zeta's*

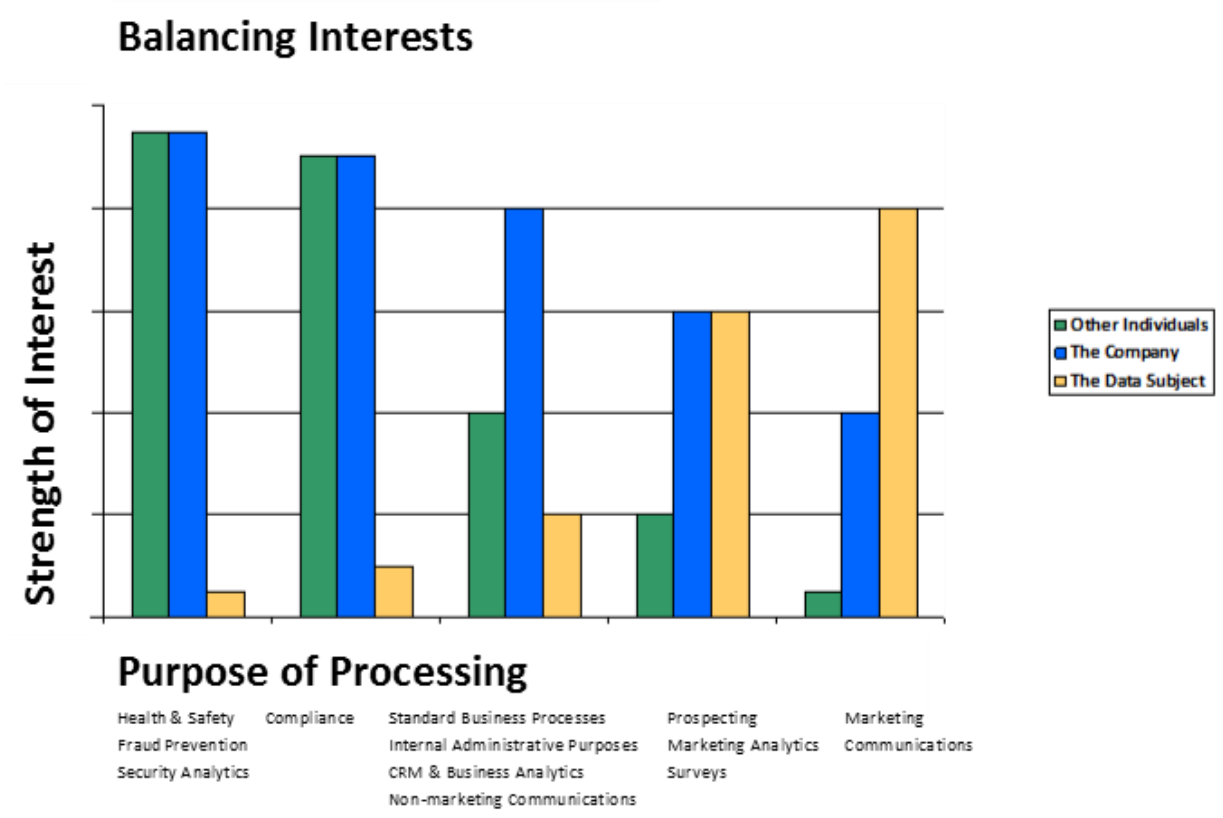
preferred customer program, inviting them to join the program. Recipients will receive a program card, with a special incentive of 100 points (equivalent to a 10€ coupon) already applied to the account. Recipients can activate their membership and use the coupon by simply providing the preferred customer number from the card while shopping in any Zeta store or online. If an individual does not use the card within one year, the reward expires and the account is flagged as inactive. No additional marketing is sent to individuals who have not activated their membership.		
Consideration of Interests:		
Controllers	***Data Subject***	***Other Individuals, Society***
As noted above, Zeta has a specific interest in developing strong relationships with Rho's customers, especially those individuals who are not currently doing business with it. By inviting those Rho customers to join its rewards program and giving them a generous incentive (10€), it may boost sales and cement relationships with its new customers.	Rho's customers have an interest in controlling the use of their data by companies, particularly with respect to marketing and relationship programs. Individuals may also find the automatic inclusion in the Zeta rewards program presumptive. However, most individuals view direct mail as unintrusive, and many people would also welcome a 10€ reward.	While other individuals do not have an interest in Zeta's marketing programs, there is a societal interest in enabling companies to effectively market their products in an appropriate manner.
Risk Mitigation: Zeta believes that the preferred customer program will be well received by most Rho's customers, and those that are not interested will not activate their account. Should individuals complain, Zeta has a process to remove the individual from program immediately.		
Conclusion: This one-time invitation enables Zeta to educate its acquired customers (from Rho) about its preferred customer program with a special incentive. Given the limits on Zeta's further use of the data (no marketing unless the account is activated by the consumer) and Zeta's process for respecting objections, the processing is justified.		

5. Sample Assessment of Processing Activities for First Party Marketing

Sample Processing Activity: *A consumer products company, Tau, offers customers the ability to opt in to receive marketing emails. Tau always sends a weekly marketing email, alerting recipients to that week's online specials. Tau also sends occasional extra emails promoting special promotions, holiday events, etc. Recipients can easily unsubscribe from the emails at any time by either clicking the link in the email or resetting their preferences in their online account. Tau's web team notices that customers occasionally put sale items in their online shopping carts but then fail to complete the transaction before the sale expires. Tau plans to send a reminder email to these customers suggesting that they complete the transaction before the sale ends.*		
Consideration of Interests:		
Controllers	***Data Subject***	***Other Individuals, Society***
Tau has a legitimate interest in encouraging its customers to	Tau's customers have the right to control the marketing	While other individuals do not have an interest in Tau's

purchase products generally, and to take advantage of promotions. Tau also has an interest in satisfying customers. Tau occasionally receives complaints from customers when they miss a sale. These complaints are handled on a case-by-case basis, but this is a labor-intensive process. Tau hopes that the emails will improve customer satisfaction and reduce costs.	communications they receive. In this case, the individuals have elected to receive marketing emails, and they may appreciate getting the additional reminder to purchase an item while it is on sale. However, the reminder emails will make it apparent that Tau is monitoring their online behavior, which may feel intrusive (or creepy) to some consumers.	marketing programs, there is a societal interest in enabling companies to effectively market their products in an appropriate manner.
Risk Mitigation: Tau's marketing team uses Privacy by Design methodologies to evaluate its email programs generally. Tau's team also carefully considers email volume and content to reduce the risk that it will send too many emails or emails that are not relevant to the recipient. In this case, because customers might not understand that Tau is monitoring their shopping carts, the team has developed a short statement that explains "What Happens When I Add an Item to My Cart?" to make it clear that Tau knows what a person has put in a cart. This statement informs customers that, if they have opted-in to emails, they may receive a reminder email if they put a sale item in the cart but do not purchase it before the sale expires. It also links to the account preference center so that any customer can change their email preferences. This statement is added to the shopping cart page and to Tau's online privacy notice. Tau's team considered allowing customers to have specific choice about the cart emails, but rejected this approach because the Tau preference management system does not have the capability to differentiate individuals who have opted-in for sale email but not for cart messages. As a result, all consumers who consent to receive sale emails will be possible recipients of the cart emails. This is clear in the privacy notice.		
Conclusion: While Tau clearly has a legitimate interest in this program, there is some risk that data subjects may be surprised or displeased by this highly targeted marketing. Tau must respect individuals' rights to object, which it will do via its email opt-out process. While the data subjects' right to object cannot practically extend to specific communications, should the cart email project prove unpopular with Tau's customers, it would reconsider its approach.		

G. Balancing Process Outcomes Depicted Visually

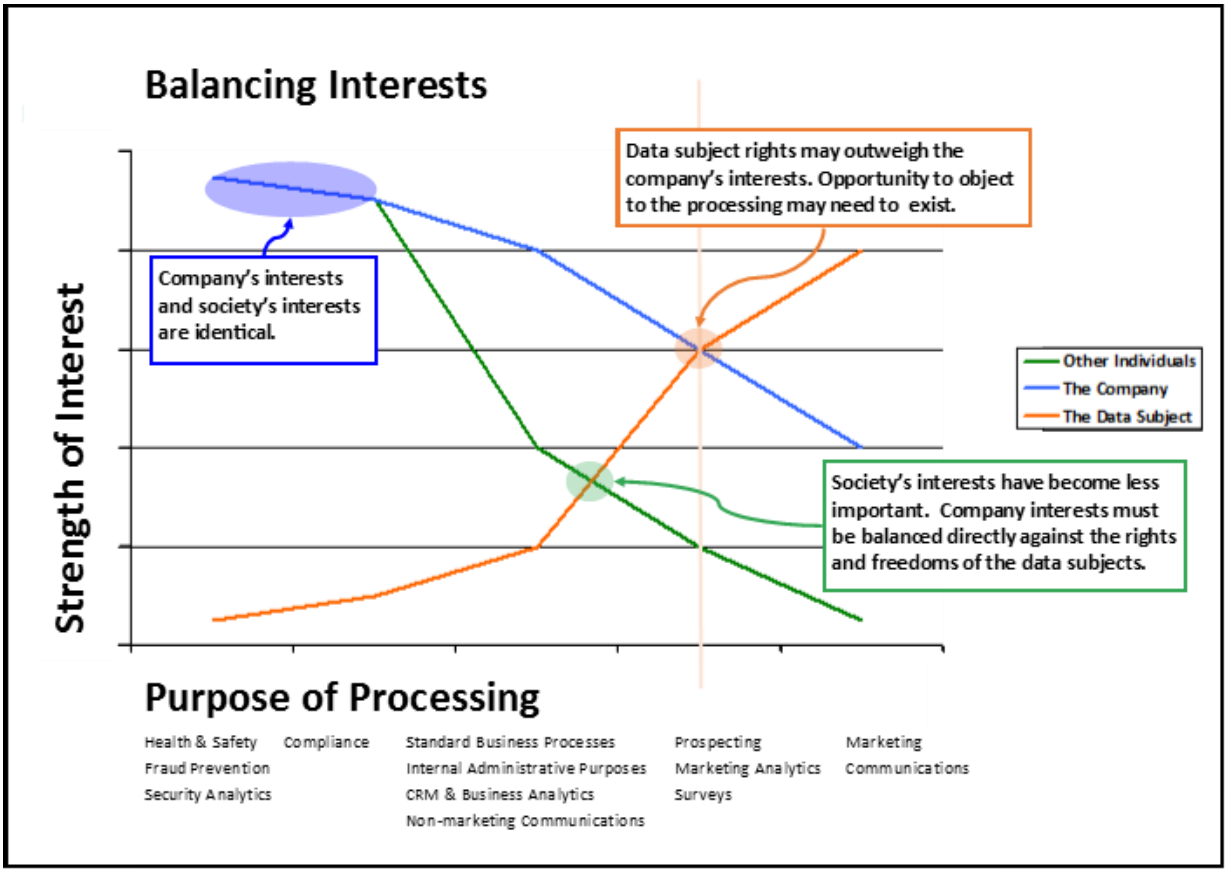


In this chart, the company's interest is reflected by the blue bar, societal interest is reflected by the green bar, and the individual data subject's interest is reflected by the yellow bar. From this depiction of relative interest, a few points become clear:

- As would be expected, both the company's interest and society's interests in processing data for health, safety, security, fraud prevention, compliance and similar functions is very high. Although the data subject certainly has an interest as well, an individual data subject's interest will rarely be so compelling as to outweigh legitimate interest that exists for these processing activities. The individual's interests must be protected by thoughtful application of the processing programs, technological controls and privacy/security by design methodologies.
- Although the societal interest is lower, companies have very compelling interests in processing data as needed to run their businesses day-to-day. While the risks to the rights and freedoms of the data subjects must be considered, the presumption must be that the processing activities are legitimate (and outweigh the interests of the individuals), provided that appropriate risk mitigation strategies are employed to prevent any unacceptable threats to the data subjects.

Farther along the spectrum, the rights and freedoms of the data subjects become more pronounced, and the ability for the individual to object to the processing becomes more important. For example, as noted in the GDPR, companies have a legitimate interest in sending marketing communications to their customers, but the rights of the individuals to object to marketing must be respected. The right to object may extend to other types of data processing, such as data collection for marketing analytics (online

behavioral tracking/targeting) and relationship communications (such as surveys). The balancing test will enable companies to determine, for any type of processing activity, how the respective interests are weighed.



We can also depict the relative interests using a traditional graph. This view is useful in that it illustrates those processing activities that are compelling both by the company's interests and by public interest.

The public interest becomes less compelling more quickly than the company's interest, however, and the point at which the individual's interest is balanced directly against the company's interests is visible. You can also see the point at which the individuals' interest begins to outweigh the company's interest, resulting in the right to object.

H. Conclusions

The ability for controllers to process personal data based on their legitimate interests is a critical component of the GDPR. An objective, easily-replicated test to enable controllers to balance the interests, rights and freedoms of all stakeholders is needed, both to ensure that risks to data subjects are managed properly but also to empower companies to engage in beneficial processing activities.

This paper is intended to provide controllers with tools to help them evaluate processing activities, using the balancing test set forth in the GDPR. It is also meant to establish objective standards regarding the types of processing activities that should be reasonably expected by all stakeholders.

Annex 1 – Processing Activities that Should Be "Reasonably Expected"

As noted above, controllers that want to process personal data based on their legitimate interests should be able to demonstrate that the data subjects reasonably expected such processing to occur.

While is it impossible to create a complete inventory of processing activities, as these will vary based on industry, context and the nature of the relationships between the controller and the individual, we can articulate many types of processing activities that are customary and reasonable. In assessing legitimate interest, these types of processing activities should be deemed "reasonably expected." This Annex is designed to provide a check-list to help controllers and authorities determine if they can easily presume that the processing activity is (or should be) "reasonably expected."

1. **Processing Needed to Protect Individuals, Organizations or the Public –** *these processing activities may also be justified as performance of a task carried out in the public interest or as necessary to protect the vital interests of the data subject or of another natural person:*

   Public Health & Safety

   - Processing for public health purposes (including identifying individuals who may been exposure to diseases, toxins, tainted food *et al.* and processing to address health risks);
   - Health-related analytics to identify and reduce adverse events, such as prescription and over-the counter pharmaceutical interactions, healthcare product or device defects and contraindications, or use/abuse of products that creates public health risk;
   - Product recalls (for hazardous products);
   - Occupational health and safety (including workplace accidents); or
   - Processing in response to natural disasters, accidents or terrorist attacks, as needed for first response, to identity victims and provide emergency services.

   Security of Networks and Information Systems
   Detecting security threats, along with processing as needed to understand, analyze and resolve the threat (including working with individuals whose systems may be compromised, sharing data with law enforcement about imminent threats or suspected criminal activity, sharing data with threat centers, identifying bad actors, improving defenses, *etc.*).

   Fraud Detection and Prevention
   Detecting and resolving fraudulent transactions; processing as needed to investigate and remediate individual claims of identity theft or misuse of their personal data or accounts.

   Security Incident & Data Breach Response ("High Risk" Incidents)
   Investigating known or suspected security incidents that might result in high risk to the impacted individuals, notifying individuals and others as may be needed to mitigate harm, other processing needed to mitigate the risk.

   Compliance with local laws and regulatory requirements
   All processing activities required to be undertaken by applicable local law. *(These processing activities would also be justified as necessary for compliance with a legal obligation to which the controller is subject in the jurisdiction where the data subject resides.)*

2. **Compliance with Laws and Regulatory Requirements from Other Jurisdictions –** *these processing activities may also be justified as necessary for compliance with a legal obligation to which the controller is subject from a jurisdiction where the controller resides, however given the potential for a conflict with the laws of the jurisdiction where the data subject resides, these obligations sit one level down on the "legitimacy spectrum."*
   - Screening required by anti-money laundering, "know your customer" and similar laws;
   - Verifying compliance with corporate policies, privacy policies and security policies, including data loss prevention controls;
   - Data sharing in response to validly-issued subpoenas or other legal requirements;
   - Maintaining ethics, compliance and whistleblower hotlines;
   - Detecting and resolving intellectual property infringement;
   - Verification and vetting of potential employees, contractors, suppliers and customers;
   - Authentication of individuals with facilities or system access, and logging access and activities for security purposes;
   - Managing premises security, such as with access controls devices (badge readers), CCTV;
   - Product recalls (non-hazardous products); or
   - Security incident response (low/no risk incidents).

3. **Standard Business Management, Internal Administrative Purposes and other functions that are directly related to the entity's relationship with the data subject**
   - Processing activities related to business transactions, assessing eligibility or credit, payment processing, fulfillment, collections, product returns, enforcing sales terms, non-marketing communications related to the transactions (such as order confirmations and shipping notices);
   - Customer service, including non-marketing communications related to customer inquiries (such as responses to questions, requests for proposals or information and complaints);
   - Loyalty and rewards programs with opt-in enrollment;
   - Corporate due diligence, such as in connection with mergers/acquisitions;
   - Recruiting potential contractors, suppliers, including issuing requests for proposals, *etc.;*
   - Customer and supplier credentialing (such as verifying eligibility or creditworthiness);
   - Corporate social responsibility programs (such as supplier diversity programs, *etc.*);
   - Quality control;
   - Data management, including data hygiene (updating records to improve accuracy) and processing for minimization, pseudonymization, anonymization, or aggregation;

- Analytics on client relationship/transactional data (complaints, returns, *et al.*) to identify process or production weaknesses, customer satisfaction, opportunities for efficiency, improvement, *etc.;*
- Product, system and application testing;
- Preference management (including managing data subject communications choices);
- Complaint handling and dispute resolution; or
- Data sharing with qualified third party processors and subprocessors.

Internal Administrative Purposes for Processing Human Resources Data:

- Customary HR data processing activities (payroll, benefits, talent, training, performance evaluation, HR services, dispute resolution *etc.);*
- Facilitating internal and external relationships between employees, and among employees and customers *et al.*;
- Corporate due diligence, such as in connection with mergers/acquisitions;
- Recruiting and evaluating prospective employees;
- Non-employment related communications to employees, such as offers of general benefits (*e.g.,* availability of flu shots, ride shares) or community service opportunities;
- Employee recognition programs;
- Corporate social responsibility program (diversity programs, equal opportunity, *etc.*);
- Data management, including data hygiene (updating records to improve accuracy) and processing for minimization, pseudonymization, anonymization, or aggregation;
- HR Analytics (such as evaluating flight risk, fairness of compensation, performance, *etc.*);
- Employee mentoring and coaching programs; or
- Data sharing with qualified third party processors and subprocessors.

4. Relationship Management, Business Intelligence, and other functions that are indirectly related to the relationship with the data subject

- Customer, consumer analytics (churn, brand, look-alike audiences, *et al.*);
- Relationship-oriented communications, such as satisfaction surveys and subscription reminders;
- Customer data enhancement, *e.g.,* for demographic analysis and segmentation;
- Analytics to determine product preferences, other predicative analytics
- Alumni networks;
- Loyalty and rewards programs with automatic enrollment; or
- Prospect identification.

5. First Party Marketing, and other functions related to establishing or expanding the relationship with the data subject

- Targeted marketing activities, including sending marketing communications via any channel and online retargeting;
- Online behavioral advertising;
- Participation in social media advertising network programs;
- Cross device tracking and targeting; or
- Promotional activities (offering and administering sweepstakes, contents, *etc.*).