Comment la Conformité au RGPD est intégrée dans les Pratiques de Gestion de Processus Métier (BPM) ?

Une revue systématique de la littérature

Jeyakumaran Sothiya[1], Rychkova Irina[2], Deneckere Rebecca[2],

1. La caisse de retraite et de prévoyance des clercs et employés de notaires.
5 Bis rue de Madrid, 75008 Paris, France
Sothiya.jeyakumaran@crpcen.fr

2. Centre de Recherches en Informatique (CRI),
Université Paris 1 - Pantheon-Sorbonne
12 Place de Panthéon, 75005, Paris, France
rebecca.deneckere@univ-paris1.fr, irina.rychkova@univ-paris1.fr

RÉSUMÉ. Le règlement général sur la protection des données (RGPD) affecte considérablement la façon dont les organisations doivent aborder la confidentialité des données, les forçant à repenser et à mettre à niveau leurs processus métiers afin de se conformer au RGPD. A travers cette revue systématique de la littérature, nous examinons les études primaires concernant cette problématique, recensons les recherches effectuées et les méthodes proposées, appliquées et intégrées dans le cycle de vie d'un processus métiers (selon BPM) pour faire face à cette nouvelle réglementation.

ABSTRACT. The General Data Protection Regulation (GDPR) dramatically affects the way organizations approach data privacy, forcing them to rethink and upgrade their business processes in order to comply with GDPR. Through this systematic literature review (SLR) we examine the primary studies, identify the research carried out and the methods that are proposed, applied and integrated into a business process life cycle (as defined by BPM) to cope with this new regulation.

Mots-clés : Règlement général sur la protection des données (RGPD) – processus métiers – revue systématique de la littérature (SLR) – cycle de vie d'un processus métiers - modélisation

KEYWORDS: General Data Protection Regulation (GDPR) - business processes - systematic literature review (SLR) - business process life cycle - modeling

DOI:10.3166/RCMA.25.1-n © 2016 Lavoisier AR_DO

1. Introduction

De nos jours, la technologie informatique permet de stocker et de traiter pratiquement toutes les informations susceptibles d'intéresser une organisation. Cependant les utilisateurs ne contrôlent pas souvent la manière dont leurs données personnelles sont collectées, stockées et traitées. Le règlement général sur la protection des données (RGPD), entré en vigueur en mai 2018, constitue une étape importante dans la direction de la protection des données personnelles (EU, 2016). Le but du RGPD est de protéger les citoyens de l'UE contre les atteintes à la vie privée de leurs données personnelles. Le RGPD contrôle la manière dont les organisations traitent les informations personnelles de leurs clients et accorde aux individus des droits de protection renforcés en ce qui concerne ces données. Les organisations non conformes au RGPD doivent faire face à de lourdes sanctions. Le RGPD présente un impact majeur sur la plupart des processus métiers des entreprises dès sa mise en œuvre. Les entreprises sont tenues de mettre en œuvre correctement les politiques de gestion des données du RGPD et de prendre les mesures appropriées sur les données lorsque leurs clients le demandent.

La conception et le développement des nouveaux systèmes d'information ainsi que l'évolution des systèmes déjà existants vers la conformité aux normes RGPD est un enjeu important pour les entreprises d'aujourd'hui. En ingénierie des SI, des solutions peuvent être apportées par un ensemble de domaines différents. Dans ce travail, nous allons nous concentrer sur un seul domaine - celui de la Gestion des Processus Métier (BPM). Les entreprises adoptent de plus en plus les systèmes de gestion de processus métiers (BPMS) afin de gérer leurs activités et la gestion des données. Ainsi, pour atteindre la conformité au RGPD, les organisations doivent remodeler leur approche de la gestion des données personnelles stockées et échangées lors de l'exécution de leurs processus métiers. Bien que la modélisation des processus métier soit bien adaptée pour exprimer la collaboration des parties prenantes et les données échangées entre les activités des processus métier et les participants, il y a peu d'études concernant la conformité du RGPD et l'identification des violations potentielles de la vie privée dans le cycle de vie d'un processus métier.

Dans cette revue systématique de la littérature (SLR) nous analysons les solutions/approches évoquées par la communauté scientifique pour la mise en conformité des processus métiers au RGPD. Les objectifs sont de (i) examiner les recherches actuelles concernant l'intégration du RGPD dans les pratiques de gestion de processus métier et notamment dans les différentes phases de cycle de vie d'un processus métier et (ii) identifier les lacunes de la recherche actuelle afin de suggérer des domaines à approfondir.

L'article est organisé de la manière suivante. La section 2 donne une définition des éléments clés de cette revue. La section 3 présente le protocole de recherche utilisé. La section 4 présente les résultats de l'analyse. Nous discuterons les résultats obtenus dans la section 5 et conclurons dans la section 6.

2. Définition des Termes Clés

Le règlement général sur la protection des données est la nouvelle loi de l'Union européenne pour la protection des données personnelles. Le RGPD définit les données

à caractère personnel comme toute information relative à une personne physique identifiée ou identifiable (“personne concernée”). Cela signifie qu'une personne concernée est une personne physique (un être humain vivant) dont les données sont gérées par un responsable du traitement (EU, 2016). Depuis 2018, le nouveau règlement a pour objectif de renforcer les droits des individus sur leurs propres données ainsi que de rendre les organisations plus responsables. Il contribue à l'harmonisation des précédentes lois fragmentées sur la protection des données à travers l'UE, afin d'assurer une protection égale des droits de l'Homme des citoyens européens.

Le RGPD définit les principes suivants concernant les données et leurs traitements : la **transparence** (les données doivent être traitées de manière équitable, licite et transparente) ; la **pertinence** (les données ne devraient être collectées qu'à des fins déterminées, explicites et légitimes, et non traitées ultérieurement à d'autres fins) ; la **minimisation** (les données traitées doivent être pertinentes, adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées) ; la **précision** (les données traitées doivent être exactes et régulièrement mises à jour) ; la **conservation** (les données doivent être supprimées après une période limitée) ; le **consentement explicite** (les données ne peuvent être collectées et traitées que si la personne donne son consentement explicite).

Les processus métiers se réfèrent généralement à toute collection structurée d'activités ou de tâches connexes effectuée pour atteindre les objectifs visés d'une organisation. Il peut être structuré en un ou plusieurs ensembles définis d'activités qui représentent les étapes nécessaires pour atteindre des objectifs relatifs aux affaires, y compris les flux et utilisations d'informations et de ressources. **La gestion des processus métier (BPM)** comprend des concepts, des méthodes et des techniques pour prendre en charge la conception, l'administration, la configuration, la mise en œuvre et l'analyse des processus métier (Weske 2010). Le cycle de vie d’un processus métier, selon BPM, est composé de 4 étapes principales : le Design (phase de modélisation où l’on réfléchit sur comment modéliser le processus métier de manière informatique afin qu’il représente de manière le plus fidèle possible la réalité), la Configuration (phase de l’implémentation où l’on met en œuvre une solution de Business process management (BPM) reliée au système d’information de l’entreprise), l’Exécution (phase opérationnelle où la solution de BPM est mise en œuvre) et l’Évaluation (phase d’analyse de l’état des processus à travers des logs, tableaux de bord détaillant la performance, etc). **BPMN** (www.omg.org) est le formalisme de représentation des processus métiers qui est la norme de facto pour la modélisation des processus. Il s'agit d'un langage riche et expressif utilisé pour les tâches associées à la modélisation des processus.

3. Protocole de Recherche

Nous avons effectué une revue systématique de littérature (Brereton et al., 2007), (Levy et Ellis, 2006). La réforme du RGPD est un sujet récent, ici nous examinons comment ce sujet est intégré par la communauté de recherche BPM au travers des outils, méthodes, théories et leurs applications dans la pratique. Nous nous sommes basées sur la méthodologie proposée par (Kichenham et Charters, 2007).

3.1. Planification et définition de questions de recherche

Cette étude vise à examiner les récentes méthodes et solutions pour la conformité des processus métiers au RGPD. Il faut savoir qu'il n'existe aujourd'hui aucune pratique standardisée du RGPD. Il est exigé que les entreprises fournissent un niveau de protection de données personnelles raisonnable mais il n'y a pas d'exigence détaillée sur la manière dont les organisations doivent mettre en œuvre le RGPD au sein de leurs processus métiers. Ainsi, les organisations doivent elles-mêmes évaluer leurs processus métiers et mettre en œuvre un plan d'action pour s'y conformer.

La question de recherche centrale (QR) est la suivante. **QR : Comment la communauté scientifique BPM envisage la conformité des processus métiers aux RGPD ?**

Nous avons développé notre étude afin de répondre aux sous-questions plus spécifiques : *QR1 : La gestion des processus métiers offre-t-elle un ensemble suffisant de méthodes et outils pour assurer la conformité au RGPD dans les organisations ?* et *QR2 : A quelles étapes du cycle de vie d'un processus métier interviennent les impacts de la conformité au RGPD ?*

De plus, nous avons examiné séparément les impacts du RGPD sur la *conception de nouveaux processus* (avec un objectif d'intégrer les normes RGPD "by design") et sur *l'évolution des processus existants* (avec un objectif d'établir la conformité aux normes plus tard dans leurs cycle de vie), ceci nous a permis de définir deux autres sous-questions : *QR3 : Comment les praticiens intègrent le RGPD dans les processus métiers existants ?* et *QR4 : Comment les normes RGPD sont intégrées à la conception du processus ?*

3.2. Étude de Sources bibliographiques

Nous avons choisi de suivre la méthode de recherche proposée par (Zhang et al., 2011) qui consiste à définir les termes et les chaînes de recherches pour la recherche automatique via les différents moteurs de recherche. Par la suite, nous avons complété par une recherche manuelle. En complétant et en évaluant dans les deux sens la recherche manuelle et la recherche automatique, il a été possible de définir un ensemble de publications pertinentes sur lesquelles nous avons effectué la technique nommée « effet boule de neige » qui repose sur les différentes références que les auteurs ont utilisées dans les publications qui constituent notre revue de littérature.

3.2.1. Recherche automatique

Les mots clefs utilisés pour la recherche reprennent les termes de "RGPD" et "Business process" avec certains synonymes de ce dernier comme "BP", "workflow", "workflow system", "Business Process System", "BPM", "Business process management". Nous avons utilisé quatre bases de données en ligne parmi les plus connues et représentatives du domaine en utilisant des chaînes de recherche à partir des syntaxes et des règles définies : IEEE Xplore, ACM Digital Library, SpringerLink et ScienceDirect (cf Tableau 1).

Nous avons ensuite établi une liste de critères à respecter pour chacun des articles à conserver pour notre étude, soit en critères d'inclusion, soit en critères d'exclusion.

Tableau 1. Résultat de la recherche automatique

Sources	Requêtes	Résultat
SpringerLink	("GDPR" OR "General Data Protection Regulation") AND ("Business process" OR "Business process system" OR "BPM" OR "BP")	145
IEEE XPLORE	((("Document Title":GDPR) OR ("Abstract":GDPR)) AND (("Abstract":Business process) OR ("Document Title":Business process)) OR (("Abstract":BPM) OR ("Document Title":BPM)))	456
ACM DIGITAL	[Publication Title: gdpr] AND [Abstract: business process] AND [Abstract: business process management] AND [Abstract: general data protection regulation]	667
ScienceDirect	("GDPR" OR "General Data Protection Regulation") AND ("Business process" OR "Business process system" OR "Business Process Management" OR "BP")	130

Critères d'inclusion : la source (a) est un article de recherche ou conférence et accessible en ligne, (b) est en anglais, (c) le titre ou le résumé est conforme aux chaînes de recherche définie, (d) fait partie des bases de données définies ci-dessus et (e) comporte une réponse de conformité RGPD au processus métier.

Tableau 2. Résultat de la recherche manuelle

Etapes	Description de l'étape	Nombre d'articles
Recherche automatique	Elaboration de la liste des sources de recherche et des requêtes de recherches	SpringerLink : 145 IEEE XPLORE : 456 ACM Digital : 667 Science Direct : 130
Premier filtrage	Application des critères d'inclusions et d'exclusions, puis lecture des articles un à un (abstract, titre et mots-clefs) pour établir le QGS.	40
Recherche « boule de neige »	Méthodes de Snowballing : on se base sur les différentes références que les auteurs ont utilisées dans les publications qui constituent notre QGS.	51 : [1] - [51]

Critères d'exclusion : la source (a) n'est pas un article scientifique (article de Blog, Magazine ou Journal grand public), (b) est antérieure à 2005, (c) ne comporte pas de résumé, (d) est une étude dupliquée et (e) s'intéresse à la conformité du RGPD sans évoquer de solutions répondant aux problèmes pour les processus métiers.

3.2.2. Recherche manuelle

Une fois la sélection terminée, tous ces articles identifiés sont utilisés pour former le quasi-gold standard. A partir de celui-ci, nous allons effectuer la méthode de l'effet boule de neige pour étendre notre bibliographie.

Suite au protocole de recherche défini, nous avons établi une liste de 51 articles afin d'effectuer notre analyse. Pour la simplicité de présentation, nous avons regroupé ces articles dans la première partie de notre bibliographie et ajouté un index numérique.

4. Extraction et Analyse des Données

Nous examinons ici l'ensemble des 51 articles sélectionnés afin de caractériser la recherche de manière quantitative et qualitative. Nous avons extrait et exploité les données sur la *date de publication*, le *thème principal*, le *type de recherche* et le *rapport avec une étape spécifique du cycle de vie du processus selon BPM*.

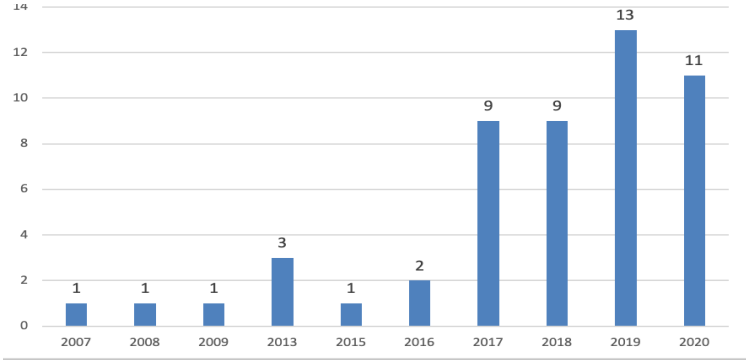

Figure 1 : Distribution des articles examinés par année de publication

La Figure 1 illustre la distribution des articles selon leur année de publication. Cette distribution démontre que l'intérêt par rapport aux problématiques de traitement de données personnelles dans le BPM a été exprimé avant l'apparition officielle du RGPD. Le nombre croissant de publications ces 3 dernières années démontre que la conformité au RGPD est un problème traité par la communauté BPM.

4.1. Classifications des articles selon des thèmes

Nous avons procédé à une lecture des articles sélectionnés et nous avons identifié 6 thèmes principaux (certains articles peuvent étudier plusieurs thèmes):

Modélisation : Ce thème comprend tous les articles présentant une méthode de modélisation, un outil de modélisation ou une proposition de modèle pour la conformité d'un processus métier au RGPD. En effet, il peut s'agir d'un outil de modélisation, de modèles existants sur le RGPD ou bien de modèles d'aide à l'élaboration de processus métiers.

Langage : Ce thème comprend principalement le langage BPMN et son évolution pour répondre à la conformité du RGPD. Ce thème comprend également les articles évoquant des langages permettant de rendre un modèle de processus conforme au RGPD.

Évaluation : Ce thème correspond à l'utilisation de méthodes et outils permettant d'évaluer les systèmes d'information des entreprises et les données afin d'élaborer des processus métiers conformes aux RGPD.

Exigences : Ce thème comprend toutes techniques et outils permettant de définir les exigences en lien avec le RGPD.

Contrôle : Ce thème comprend les méthodes et outils permettant de faire des contrôles sur les processus existants.

Exploration : Ce dernier thème comprend principalement les méthodes de fouille de processus au service du RGPD et des processus métiers.

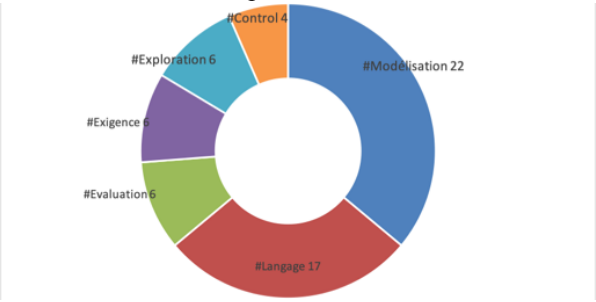

Figure 2 : Résultat de la classification par thème.

D'après nos résultats, le thème comportant le plus d'articles est « Modélisation » (22 articles). Plusieurs articles évoquent des solutions ou méthodes de modélisation (autres que BPMN) visant la conformité des PM aux RGPD. Certains articles proposent des modèles de conceptions de PM propres à chaque contrainte du RGPD. D'autres articles proposent des modèles UML ou modèles de conception d'aide à la modélisation - des modèles représentant les différentes contraintes du RGPD pour une meilleure compréhension des relations des diverses contraintes.

« Langages » est le deuxième thème le plus évoqué (17 articles). Une majorité d'articles évoque la conformité des processus métiers au RGPD via l'évolution du BPMN. BPMN est le formalisme le plus couramment utilisé pour représenter les processus métiers. BPMN est conçu pour être un langage extensible, il peut être utilisé pour créer des extensions pour de nouveaux artefacts dans les diagrammes BPMN. Un large nombre d'articles propose des solutions d'extensions de BPMN pour représenter les tâches liées à la protection des données. La deuxième solution la plus évoquée dans ce thème vise à intégrer le modèle juridique du RGPD dans un processus métier. Par exemple, le modèle DAPRECO [25][32][38] propose un formalisme et définit un référentiel de règles RGPD écrites en LegalRuleML - un standard pour représenter le contenu sémantique et logique des documents juridiques.

« Exploration », « Évaluation » et « Exigences » sont représentés par 6 articles chacun. Ces 3 thèmes présentent des solutions évoquées dans la mise à place de la conformité au RGPD des processus métiers. Concernant l'exploration, les solutions évoquées concernent la méthode de la fouille de processus. En effet, il s'agit d'explorer les logs des processus métiers pour viser la conformité du RGPD. Pour le thème de l'évaluation, les articles évoquent des méthodes d'évaluation des systèmes d'information par les acteurs afin d'élaborer des PM adaptés aux contraintes du RGPD. Et enfin le dernier thème concerne les exigences et les articles évoquent plus

précisément les exigences de sécurité et de confidentialité En effet, les articles proposent des méthodes afin d'analyser ses exigences pour une meilleure compréhension de celles-ci afin de permettre une conception de PM plus efficace.

Le thème le moins évoqué par notre liste de sources est le thème du « Contrôle » (4 articles). Les seuls contrôles proposés concernant les processus métiers existants concernent les contrôles d'accès et d'habilitation afin d'effectuer des contrôles sur chaque activité exécutée.

Tableau 3. Analyse selon le thème

Thème	**Articles du SLR**
Modélisation	[1][3][4][5][7][8][11][13][14][15][17][22][23][24][26][31][32][33][42][44][47][48]
Langage	[1][2][5][6][14][19][21][30][35][36][37][38][39][40][42][43][47]
Évaluation	[2][4][18][25][34][45]
Exigences	[10][15][27][28][37][46]
Contrôle	[12][16][33][41]
Exploration	[9][20][29][49][50][51]

4.2. Classification des articles selon le type de recherche

Nous avons établi 3 types d'articles selon le type de recherche utilisée :

Recherche théorique : Ce type d'article a pour objectif d'établir une problématique ou question de recherche afin d'y répondre en déterminant les concepts clefs, les théories et les idées préexistantes en lien avec le sujet choisi sans proposer de solutions pratiques.

Recherche proposant une solution sans validation empirique : Ce type d'article consiste en une proposition de solutions à un problème ou question de recherche défini sans validation empirique c'est-à-dire aucune preuve d'observation ou d'expérimentation pour la solution proposée.

Recherche proposant une solution avec validation empirique : par ce type, nous avons regroupé les articles proposant une solution à un problème ou question de recherche défini avec une validation/preuve empirique (des exemples de cas pratiques, des expérimentations sont évoqués dans les articles).

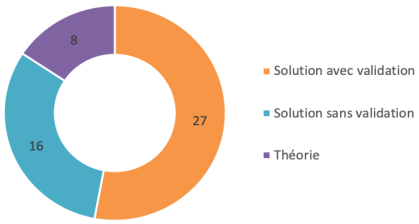

Figure 3. Résultat de la classification par type de recherche

Des “recherches proposant une solution avec validation empirique” sont présentées dans 27 articles. Parmi les travaux examinés, un grand nombre d'articles proposent des solutions pour la conformité des processus métiers au RGPD avec des preuves empiriques. Ces preuves sont principalement des démonstrations suite à des observations/expérimentations ou des validations par les pairs. Ces articles sont également accompagnés de cas pratiques pour démontrer les solutions proposées. Ainsi, ils proposent non seulement un aspect théorique avec une approche ou méthodologie bien définie mais également un aspect pratique en démontrant la mise en œuvre de leurs solutions et analysant les observations et résultats obtenus.

Tableau 4. Analyse selon le type de recherche

Type	**Articles du SLR**
Recherche théorique	[13][25][29][32][34][38][41][46]
Recherche proposant une solution sans validation empirique	[1][3][8][10][14][15][17][21][22][27][31][33][39][44][45][50]
Recherche proposant une solution avec validation empirique	[2][4][5][6][7][9][11][12][16][18][19][20][23][24][26][28][30][35] [36][37][40][42][43][47][48][49][51]

4.1.3. Classification selon l’étape du cycle de vie d’un Processus Métier (d'après BPM)

16 articles présentent des “recherches proposant une solution sans validation”. Ces articles présentent des solutions qui ne sont pas (encore) implémentées ou validées ; aucune analyse des observations ou résultats obtenus suite à la mise en œuvre n’est évoquée.

Finalement, 8 articles présentent des “recherches théoriques”. Ce qui correspond bien à la nature très appliquée du sujet (conformité au RGPD). Ces articles ont principalement pour objectif de définir les concepts clefs et théories concernant les contraintes du RGPD et l’impact au niveau des processus métiers.

L’objectif de cette analyse est d’identifier les étapes du cycle de vie du PM comportant le plus grand nombre d’études et de recherches concernant la conformité au RGPD mais également en identifiant les étapes comportant des lacunes, un manque de recherche ou ne comportant pas de solutions bien définies. Les quatre étapes du cycle de vie d’un PM sont le Design, la Configuration, l’Exécution et l’Évaluation.

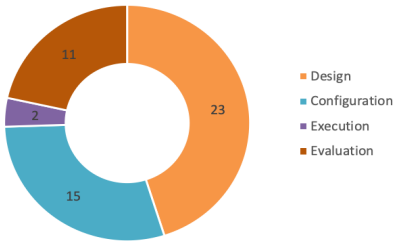

Figure 4. Résultat de la classification par étape du cycle de vie selon BPM

Le "*Design*" est l'étape la plus présentée par les articles scientifiques (23 articles). Les chercheurs proposent un grand nombre de modèles de PM conformes aux contraintes du RPGD. La notion de conformité s'articule autour de la notion de but / finalité. [12] propose d'associer les processus métiers avec un ou plusieurs objectifs permettant d'identifier les finalités et de classer les types de données collectées, en conformité avec le RGPD. [44] présente un modèle conceptuel du RGPD qui intervient comme un outil d'aide à la modélisation de processus métiers. C'est un outil pour aider à l'élaboration d'une politique de confidentialité organisationnelle. L'objectif est de l'utiliser comme un cadre de référence pour conduire la définition des règles de confidentialité car il fournit une vue d'ensemble pratique mais concrète du RGPD. En comprenant l'état existant des activités de traitement des données dans une organisation et en les instanciant dans le modèle, les zones de conformité partielle ou de non-conformité peuvent être identifiées à partir desquelles des politiques internes peuvent être construites et même renforcées et des actions peuvent être menées au niveau de l'élaboration des processus métiers. Une autre application potentielle de ce modèle peut être le développement d'extensions de langages de modélisation conformes au RGPD. [3] évoque les 7 principales contraintes du RGPD et un processus métier est défini pour chacun d'eux grâce aux langages BPMN.

L'étape de "*Configuration*" est considérée par 15 articles. Cette étape permet de s'intéresser à la configuration que nous pouvons mettre en place pour mettre en œuvre le processus métier (ressources organisationnelles, composants SI). L'intégration directe des exigences du RGPD dans la configuration et par la suite à l'exécution des processus métier représente un aspect clé à la fois pour la gestion de la confidentialité et la validation pour les entreprises. [11] et [19] proposent une approche qui utilise le modèle juridique du RGPD pour enrichir un processus métier d'annotations qui expriment des exigences de protection des données.

L'étape "*d'Évaluation*" est prise en compte par 11 articles. Ces articles évoquent principalement des techniques et méthodes d'analyse à partir des logs existants pour analyser les processus métiers et être conforme au RGPD. Une grande majorité des articles évoquent la nécessité de revoir la conception des processus métiers suite à l'analyse. [29][49][50] évoquent une solution de conformité RGPD orientée entreprise en se basant sur l'utilisation de fouille de processus (process mining). [29] prévoit d'utiliser et d'améliorer les techniques de fouille de processus pour résoudre les problèmes tels que le contrôle de conformité des processus métiers.

L'étape "*d'Exécution*" est présentée dans 2 articles. Les auteurs de [16] proposent une intégration directe des exigences du RGPD dans l'exécution des processus métiers via l'utilisation de services de sécurité tels que les contrôles d'accès. Cela peut représenter un aspect clé à la fois pour la gestion et l'assurance de la confidentialité. Le faible nombre d'articles centrés sur cette étape du cycle de vie peut indiquer que le retour d'expérience et les solutions pour une analyse de conformité RGPD en "run time" sont toujours en cours de développement.

Nous pouvons conclure que la communauté considère que l'élaboration d'un nouveau processus métier reste pour le moment une solution plus efficace pour répondre à la conformité du RGPD par rapport à l'évolution d'un processus déjà existant.

Tableau 5. Analyse selon la phase du cycle de vie

Phase	**Articles du SLR**
Design	[3][7][8][10][11][12][13][15][17][22][23][24][26][27][28][31][32][33][36][44][46][47][48]
Configuration	[1][2][5][6][14][19][21][30][35][37][38][39][40][42][43]
Exécution	[16][41]
Évaluation	[4][9][18][20][25][29][34][45][49][50][51]

5. Discussion

Suite à notre analyse, nous pouvons répondre à nos questions de recherche définies pour cette étude : **Comment la communauté scientifique BPM envisage la conformité des processus métiers aux RGPD ?**

QR1 : La gestion des processus métiers offre-t-elle un ensemble suffisant de méthodes et outils pour assurer la conformité au RGPD dans les organisations ?
Beaucoup de publications (Figure 1) illustrent un grand intérêt de la communauté scientifique BPM pour le sujet de protection de données. Les techniques et les méthodes de modélisation, d'analyse et d'évaluation de processus métiers sont considérées comme des outils des plus importants pour les entreprises afin d'assurer la conformité au RGPD. La plupart des contributions scientifiques étudiées proposent des solutions pratiques (avec ou sans validation) - ce qui illustre une grande valeur appliquée (Figure 3).

QR2 : A quelles étapes du cycle de vie interviennent les impacts de la conformité au RGPD ?
Toutes les étapes du cycle de vie d'un processus métier sont concernées par la conformité du RGPD et représentées par les articles de recherche (Figure 4). Il est important d'initier les processus métiers conformes au RGDP mais également de surveiller le fonctionnement et le flux des données dans la phase d'évaluation. Dans la classification par thème de l'analyse quantitative, les étapes les plus approfondies qui ont été remontées sont les étapes de design et de la configuration.

QR3 : Comment les praticiens intègrent le RGPD dans les processus métiers existants ?
D'après notre étude, peu de recherches rapportent des résultats sur des processus métiers déjà existants (étape d'exécution) et leur mise en conformité "at run time" (Figure 4). Certaines contributions sont axées sur le Contrôle et l'Exploration (Figure 2), où la conformité (ou l'absence de conformité) au RGPD peut être détectée en utilisant des techniques de fouille de processus.

QR4 : Comment les normes RGPD sont intégrées à la conception du processus ?
Le "Design" est l'étape la plus alimentée par la communauté scientifique (Figure 4). Elle comporte un nombre important de solutions pertinentes et d'aide à la modélisation des processus métiers conformes au RGPD. L'intérêt pour cette étape peut s'expliquer par l'effet qu'elle comporte un coût budgétaire plus faible. En effet, la prise en compte du RGPD dès le départ permet d'éviter plusieurs difficultés telles que le fait de retravailler sur plusieurs points du projet nécessitant la conformité qui peuvent impliquer des coûts supplémentaires mais également un retard dans la mise en production. De plus,

lorsque la conformité est prise en compte dès le démarrage, le risque de poursuites judiciaires pour cause de manquement est réduit comparé à la mise en place de la conformité sur des processus existants.

En examinant les différentes étapes de cycle de vie BPM, nous avons identifié les deux étapes les plus impactées par RGPD: l'étape de Design où la communauté scientifique cherche à assurer la conformité RGPD en amont, par des technique de modélisations et d'analyse de modèles; et l'étape d'Évolution, où la communauté cherche à valider la conformité RGPD en aval, par exemple par des techniques de fouille de processus.

La communauté scientifique envisage le BPMN comme un langage adéquat pour viser la conformité du RGPD. Un grand nombre d'articles évoquent des solutions d'évolution du BPMN pour représenter les processus métiers. Suite à l'exécution des processus métiers, les méthodes d'explorations sont soulevées par certains articles pour surveiller et contrôler la conformité des processus métiers. L'objectif étant de s'assurer que les processus métiers liés au RGPD soient continuellement surveillés. Les écarts entre les processus modélisés et les traces générées par les journaux doivent être identifiés, optimisés et initier les changements des processus futurs conformes au RGPD.

Les techniques de fouille de processus sont très efficaces pour évaluer les processus métiers et envisager une re-conception après avoir fait une analyse des violations existantes dans le processus métier. L'objectif étant d'effectuer un suivi des processus liés au RGPD. Les étapes de surveillance sont très importantes pour les entreprises, car depuis la mise en place du RGPD, les entreprises ont l'obligation de prouver qu'elles se conforment à celui-ci. Ainsi, les logs et les techniques de fouille de processus permettent d'établir les preuves nécessaires (données supprimées, accès, finalités, etc.).

6. Conclusion

Traditionnellement, n'ayant pas d'obligation en place, les organisations et les entreprises traitent les données personnelles de personnes, dans quelques cas sans consentement explicite, avec des finalités d'utilisation non définies, les conservant pour des périodes illimitées et même les sous-louant à d'autres entreprises. Le règlement européen sur la protection des données impose depuis le 25 mai 2018 de nouvelles contraintes aux entreprises concernant le traitement des données à caractère personnel. Par conséquent, cela engendre de grands changements organisationnels comme le déploiement de personnes dédiées à la protection des données, la modification des politiques d'accès aux données, la formation du personnel pour améliorer la culture et la sensibilisation à la confidentialité, des modifications techniques comme la mise à jour des processus métiers.

Le RGPD influence fortement la façon dont les organisations doivent aborder la confidentialité des données, les forçant à repenser et à mettre à niveau leurs processus métiers afin de s'y conformer. Pour de nombreuses organisations, cela peut être une tâche complexe, car jusqu'à présent, très peu de travaux ont été réalisés pour identifier facilement les problèmes de confidentialité dans les processus métiers. Notre étude avait pour but d'examiner cette problématique afin de faire ressortir les solutions envisagées, les avantages et les limites des recherches scientifiques sur la conformité des processus

métiers au RGPD. Nous avons effectué un focus sur chaque étape du cycle de vie d'un processus métier afin d'y observer les recherches menées jusqu'à aujourd'hui. Nous constatons que la conformité est à prendre en compte dans toutes les étapes du cycle de vie d'un processus métier, notamment les étapes de modélisation et de configuration. Certaines recherches proposent des solutions alternatives dans les deux autres phases comme les contrôles d'accès ou la fouille de processus. Il est à noter que 40% des articles ne présentent pas de preuves empiriques et/ou solutions de mise en œuvre. En effet, l'entrée en vigueur du RGPD datant de 2018, les recherches concernant la conformité des processus métiers au RGPD n'en sont qu'à leurs débuts.

Par conséquent, l'objectif d'un grand nombre de chercheurs est de mettre en œuvre ces solutions afin d'analyser les résultats obtenus et d'effectuer une validation de la solution. Une fois avoir validé la solution, il s'agira d'établir une approche pour la mise en œuvre de celle-ci dans les entreprises. De plus, un deuxième domaine peu évoqué mais pouvant être intéressant dans les travaux futurs concerne le transfert des données à des tiers. Le RGPD a des règles précises concernant les acteurs qui peuvent transférer des données à d'autres parties, quand ces transferts peuvent avoir lieu et dans quelles circonstances les autres parties peuvent ou doivent supprimer, produire ou stocker des données. Ainsi, il serait intéressant de proposer des solutions pour les entreprises sur cet aspect du RGPD qui est peu évoqué actuellement.

Pour finir, ce présent travail est une étape préliminaire pour recenser les solutions visant la conformité des processus métiers au RGPD. Afin de poursuivre ce travail, il serait pertinent de s'intéresser également (a) au RGPD en amont des processus en se focalisant sur l'impact du règlement sur l'ingénierie des exigences et (b) à l'aspect infrastructure impactée par le RGPD, ainsi qu'aux problématiques de circulation et de stockage des données concernées. Nous souhaitons également étudier la mise en œuvre des solutions proposées par la communauté scientifique sur des cas pratiques réels pour les entreprises.

Bibliographie utilisée dans la revue systématique de la littérature

1. (Agarwal et al., 2017) Agarwal S., Kirrane S., Scharf J. (2017). Modelling the general data protection regulation. Internationales Rechtsinformatik Symposion (IRIS)
2. (Agarwal et al., 2018) Agarwal S., Steyskal S., Antunovic F., Kirrane S. (2018) Legislative Compliance Assessment: Framework, Model and GDPR Instantiation. Annual Privacy Forum (APF 2018), Barcelona, Spain
3. (Agostinelli et al., 2019) Agostinelli S., Maggi F.M., Marrella A., Sapio F. (2019) Achieving GDPR Compliance of BPMN Process Models. Information Systems Engineering in Responsible Information Systems (CAiSE 2019) Lecture Notes in Business Information Processing, vol 350. Springer, Cham.
4. (Ahmadian et al., 2018) Ahmadian A., Strüber D., Riediger V., Jürjens J. (2018). Supporting privacy impact assessment by model-based privacy analysis. Annual ACM Symposium on Applied Computing (SAC '18), pp 1467–1474
5. (Ahmed et Matulevičius, 2014) Ahmed N., Matulevičius R. (2014). Securing Business Processes using Security Risk-oriented Patterns. Computer Standards & Interfaces. Vol 36, Issue 4, pp 723-733
6. (Altuhhova et al., 2013) Altuhhova O., Matulevičius R., Ahmed N. (2013) An Extension of Business Process Model and Notation for Security Risk Management. International Journal of Information System Modeling and Design.

7. (Antignac et al., 2016) Antignac T., Scandariato R., Schneider G. (2016) A Privacy-Aware Conceptual Model for Handling Personal Data. Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques. ISoLA 2016.
8. (Arba et Arba, 2019) Arba R. et Arba A. (2019) Business Process Modeling of a GDPR Compliant System for Research Project Management. Journal of Applied Computer Science & Mathematics. 13(2):14-18
9. (Arfelt et al., 2019) Arfelt E., Basin D., Debois S. (2019) Monitoring the GDPR. Computer Security – ESORICS 2019. Lecture Notes in Computer Science, vol 11735. Springer, Cham.
10. (Bartolini et al., 2017) Bartolini C., Muthuri R., Santos C. (2017) Using Ontologies to Model Data Protection Requirements in Workflows. New Frontiers in Artificial Intelligence (JSAI-isAI 2015). Lecture Notes in Computer Science, vol 10091. Springer, Cham
11. (Bartolini et al., 2019) Bartolini C. Calabrò A. Marchetti E. (2019). Enhancing Business Process Modelling with Data Protection Compliance: An Ontology-based Proposal. International Conference on Information Systems Security and Privacy. 421-428.
12. (Basin et al., 2018) Basin D., Debois S., Hildebrandt T. (2018) On Purpose and by Necessity: Compliance Under the GDPR. Financial Cryptography and Data Security (FC 2018). Lecture Notes in Computer Science, vol 10957.
13. (Besik et Freytag, 2020) Besik, S. I., & Freytag, J. C. (2020). Managing Consent in Workflows under GDPR. In ZEUS (pp. 18-25).
14. (Bonatti et al., 2020) Bonatti P.A., Kirrane S., Petrova I.M., Sauro L. (2020). Machine Understandable Policies and GDPR Compliance Checking. KI - Künstliche Intelligenz, vol. 34, pp. 303-315
15. (Buchmann et al., 2017) Buchmann E., Anke J. (2017). Privacy Patterns in Business Processes. Jahrestagung der Gesellschaft für Informatik (Informatik 2017), Germany
16. (Calabrò et al., 2019) Calabrò, A., Daoudagh, S., Marchetti, E. (2019) Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study. Italian conference on Cyber Security (ITASEC 2019).
17. (Capodieci et Mainetti, 2020) Capodieci A., Mainetti L. (2020) A Structured Approach to GDPR Compliance. Digital Transformation of Collaboration (COINs 2019). Springer Proceedings in Complexity. Springer, Cham.
18. (Capodieci et Mainetti, 2019) Capodieci A., Mainetti L. (2019) Business process awareness to support GDPR compliance. International Conference on Information Systems and Technologies (ICIST 2019).
19. (Bartolini et al., 2019) Bartolini C., Calabrò A., Marchetti E. (2019). GDPR and business processes: an effective solution. International Conference on Applications of Intelligent Systems (APPIS'19). 1-5.
20. (Chitanut et Sotarat, 2020) Chitanut T., Sotarat T. (2020) A Data Masking Guideline for Optimizing Insights and Privacy Under GDPR Compliance. International Conference on Advances in Information Technology (IAIT2020). Association for Computing Machinery, New York, NY, USA, 22, pp. 1–9.
21. (Gerl and Meier, 2019) Gerl A., Meier B. (2019) The Layered Privacy Language Art. 12 – 14 GDPR Extension – Privacy Enhancing User Interfaces . Datenschutz Datensich. Vol. 43, pp 747–752.
22. (Gonçalves et al., 2017) Gonçalves A., Correia A., Cavique L. (2017) Data Protection Risk Modeling into Business Process Analysis. Computational Science and Its Applications (ICCSA 2017)
23. (Heuck et al., 2017) Heuck E., Hildebrandt T.,Lerche R., Marquard M., Normann H., Strømsted R.,Weber B. (2017) Digitalising the General Data Protection Regulation with Dynamic Condition Response Graphs. BPMN 2017.
24. (Kühnel et Zasada, 2018) Kühnel S. Zasada A. (2018). An Approach Toward the Economic Assessment of Business Process Compliance. Lecture Notes in Computer Science. pp 228-238.

25. (Lioudakis et al., 2020) Lioudakis G.V., Koukovini M.N., Papagiannakopoulou E.I., Dellas N., Kalaboukas K., Medeiros de Carvalho R., Hassani M., Bracciale L., Bianchi G., Juan-Verdejo A., Alexakis S., Gaudino F., Cascone D., Barracano P. (2020) Facilitating GDPR Compliance: The H2020 BPR4GDPR Approach. Digital Transformation for a Sustainable Society in the 21st Century. IFIP Advances in Information and Communication Technology, vol 573. Springer, Cham.
26. (Matulevičius et al., 2020) Matulevičius R., Tom J., Kala K., Sing E. (2020) A Method for Managing GDPR Compliance in Business Processes. Advanced Information Systems Engineering (CAiSE 2020).
27. (Matulevičius et Ahmed, 2013) Matulevičius R., Ahmed N. (2013). Eliciting Security Requirements from the Business Processes Using Security Risk-Oriented Patterns. Information Technology.
28. (Menzel et al., 2009) Menzel M., Thomas I., Meinel C. (2009). Security Requirements Specification in Service-Oriented Business Process Management. International Conference on Availability, Reliability and Security (ARES 2009). pp. 41 - 48.
29. (Mozafari Mehr, 2019) Mozafari Mehr A. (2019) Compliance to data protection and purpose control using process mining technique. BPM Doctoral Consortium 2019: International Conference on Business Process Management, pp. 108-113.
30. (Notario et al., 2017) Notario N., Ciceri E., Crespo A., Real E., Catallo I., Vicini S. (2017). Orchestrating Privacy Enhancing Technologies and Services with BPM Tools: The WITDOM Data Protection Orchestrator. International Conference on Availability, Reliability and Security (RES '17). No.: 89 pp. 1–7
31. (Palmirani et Governatori, 2018) Palmirani M., Governatori G. (2018) Modelling Legal Knowledge for GDPR Compliance Checking. Frontiers in Artificial Intelligence and Applications, Vol. 313: Legal Knowledge and Information Systems
32. (Palmirani et al., 2018) Palmirani M., Martoni M., Rossi A., Bartolini C., Robaldo L. (2018) Legal Ontology for Modelling GDPR Concepts and Norms. Frontiers in Artificial Intelligence and Applications, Vol. 313: Legal Knowledge and Information Systems.
33. (Pilipchuk et al., 2018) Pilipchuk R., Seifermann S., Heinrich R. (2018) Aligning Business Process Access Control Policies with Enterprise Architecture. Central European Cybersecurity Conference, pp. 1-4.
34. (Priyadharshini et Shyamala, 2018) Priyadharshini G., Shyamala K. (2018) Strategy and Solution to comply with GDPR : Guideline to comply major articles and save penalty from non-compliance. International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC 2018), pp. 190-195.
35. (Pullonen et al., 2017) Pullonen P., Matulevičius R., Bogdanov D. (2017) PE-BPMN: Privacy-Enhanced Business Process Model and Notation. Business Process Management (BPM 2017). Lecture Notes in Computer Science, vol 10445.
36. (Pullonen et al., 2019) Pullonen, P., Tom, J., Matulevičius, R. et al. Privacy-enhanced BPMN: enabling data privacy analysis in business processes models. Softw Syst Model 18, 3235–3264 (2019). https://doi.org/10.1007/s10270-019-00718-z
37. (Ramadan et al., 2020) Ramadan, Q., Strüber, D., Salnitri, M., Jürjens J., Riediger V., Staab S. (2020) A semi-automated BPMN-based framework for detecting conflicts between security, data-minimization, and fairness requirements. Software System Model. vol 19.
38. (Robaldo et al., 2019) Robaldo L., Bartolini C., Palmirani M., Rossi A., Martoni M., Lenzini G. (2019) Formalizing GDPR Provisions in Reified I/O Logic: The DAPRECO Knowledge Base. Journal of Logic Language and Information. 29, pp 401–449.
39. (Robol et al., 2017) Robol M. Salnitri M., Giorgini P. (2017). Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework. IFIP Working Conference on The Practice of Enterprise Modeling. pp. 236-250.

40. (Rodriguez et al., 2007) Rodriguez A., Fernández-Medina E., Piattini M. (2007). A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE Transactions on Information and Systems. E90D. 10.1093/ietisy/e90-d.4.745.
41. (Roosendaal, 2020) Roosendaal A. (2020) DPIAs in practice – a strategic instrument for compliance . Datenschutz Datensich. vol. 44, pp. 166–168
42. (Salnitri et al., 2017) Salnitri, M., Dalpiaz, F., Giorgini, P. (2017) Designing secure business processes with SecBPMN. Software System Model. 16, 737–757.
43. (Sang et al., 2015) Sang K.S., Zhou B. (2015) BPMN Security Extensions for Healthcare Process, IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, pp. 2340-2345,
44. (Tom et al., 2018) Tom J., Sing E., Matulevičius R. (2018) Conceptual Representation of the GDPR: Model and Application Directions. Perspectives in Business Informatics Research (BIR 2018) Lecture Notes in Business Information Processing, vol 330. Springer.
45. (Toots et al., 2019) Toots A., Tuuling R., Yerokhin M., Dumas M., García-Bañuelos L., Laud P., Matulevičius R., Pankova A., Pettai M. Pullonen P., Tom J. (2019) Business Process Privacy Analysis in Pleak. Fundamental Approaches to Software Engineering (FASE 2019). Lecture Notes in Computer Science, vol 11424. Springer, Cham.
46. (Voglhofer and Rinderle-Ma, 2020) Voglhofer T., Rinderle-Ma S. (2020) Collection and Elicitation of Business Process Compliance Patterns with Focus on Data Aspects. Business and Information Systems Engineering, vol. 62, pp. 361–377
47. (Winter et al., 2020) Winter, K., van der Aa, H., Rinderle-Ma, S., & Weidlich, M. (2020). Assessing the Compliance of Business Process Models with Regulatory Documents. In International Conference on Conceptual Modeling (pp. 189-203). Springer, Cham.
48. (Wolter et al., 2008) Wolter C., Menzel M., Meinel C. (2008). Modelling Security Goals in Business Processes.. Modellierung 2008. pp. 197-212.
49. (Zaman et al., 2019) Zaman R., Cuzzocrea A., Hassani M. (2019) An Innovative Online Process Mining Framework for Supporting Incremental GDPR Compliance of Business Processes. IEEE International Conference on Big Data (Big Data), pp. 2982-2991,
50. (Zaman et Hassani, 2019) Zaman R., Hassani M. (2019). Process mining meets GDPR compliance: the right to be forgotten as a use case. ICPM Doctoral Consortium 2019
51. (Zaman et Hassani, 2020) Zaman R., Hassani M. (2020) On Enabling GDPR Compliance in Business Processes Through Data-Driven Solutions. SN COMPUT. SCI. vol. 1, pp. 210

Bibliographie utilisée dans l'article

(Kichenham et Charters, 2007) Kitchenham B.A., Charters S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering.

(Zhang et al., 2011) Zhang H. Ali Babar M. Tell P. (2011) Identifying relevant studies in software engineering. Information & Software Technology. vol.53, pp. 625-637.

(Brereton et al., 2007) Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. Journal of systems and software, 80(4), 571-583.

(Levy et Ellis, 2006) Levy, Y., Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research.

(Weske, 2010) Weske M. (2010). Business Process Management: Concepts, Languages, Architectures (1st. ed.). Springer Publishing Company, Incorporated.

(EU, 2016) Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/oj