4 March 2024

European Commission

Mr John Berrigan

Director General

Directorate-General for Financial Stability, Financial Services and Capital Markets Union

Rue de Spa 2 / Spastraat 2, 1000 Brussels

By e-mail: John.berrigan@ec.europa.eu

Belgian presidency of the Council of the European Union

Theodora Gentzis

President of the Board of Directors of the FPS Foreign Affairs, Foreign Trade and Development Cooperation

+32 2 501 45 84

By e-mail: pcd.pa@diplobel.fed.be

Hendrik Van de Velde

General coordinator

By e-mail: EU2024helpcenter@diplobel.fed.be

Berbel Baert

Operations coordinator

+32 2 423 26 24

By e-mail: EU2024helpcenter@diplobel.fed.be

Laurens Soenen

Communications coordinator

+32 471 30 11 90

By e-mail: commEU2024BE@diplobel.fed.be

EU Proposal for a regulation on a framework for Financial Data Access (FIDA)

Dear Mr Berrigan, dear Ms Gentzis, dear Mr Van de Velde, dear Ms Baert, dear Mr Soenen,

The European Financial Markets Lawyers Group (the "**EFMLG**") is a group of senior legal experts from the EU banking sector dedicated to making analysis and undertaking initiatives intended to foster the harmonization of laws and market practices and facilitate the integration of financial markets in Europe. The members of the

Group are selected on the basis of their personal experience amongst lawyers of major credit institutions based in the EU active in the European financial markets. The Group is hosted by the European Central Bank.

Introduction

The EFMLG acknowledges that the digital economy can be a source of growth for the EU economy. Therefore, it appreciates the related EU policies in the financial space the purpose of which is to create a European financial data space based on a broad set of regulatory measures, such as the Data Act[1], the Digital Markets Act ("DMA")[2], the Data Governance Act[3] and the recently proposed Framework for a Financial Data Access ("FIDA").

The latest proposal is meant to create a governance environment for data sharing, that protects and empowers consumers, as well as promotes data-enabled financial products and services, thus enhancing. competition with the offer of a new range of financial services by entities under its scope.

While FIDA is without a doubt a very innovative framework with merit, it also exhibits some points of serious concern for the banking sector, as described below.

On a positive note, we recognize and appreciate that the European Commission ("Commission") has considered the concerns highlighted by the banking sector during the consultation phase about the need to provide for a compensation mechanism for data sharing by the data holder, about alignment with the General Data Protection Regulation ("GDPR")[4] and the need to receive explicit prior consumer permission to share data.

However, we believe that the proposal is quite ambitious in terms of range of data to be shared, entities within its scope and timeline for its implementation, as well as vague in respect of some of its terms. The new wide data sharing obligations, which basically cover the majority of customer data held by banks, could entail significant compliance costs and deepen the asymmetry in data sharing (introduced by the Payment Services Directive ("PSD2")[5]) with respect to other sectors.

Therefore, and to avoid a potential disruptive effect on the EU banking business model, the proposal would benefit from a further impact analysis that could include the following aspects:

- Quantitative impact assessment on the benefits for the EU economy. The Commission acknowledged that "*given the limited availability of data it was inherently difficult to make quantitative predictions about the benefits on the EU economy as a whole*". However, adopting such an innovative proposal without a proper quantitative assessment is an unexpected move in light of the EU principles of better regulation. In particular, the cost of implementation for data holders should be taken into consideration and be balanced against any benefits. A quantitative in-depth impact study clearly showing benefits for the EU economy should be a pre-requisite for any further activity.

[1] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).
[2] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).
[3] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
[4] 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).
[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

- Quantitative impact assessment on the potential impact on financial intermediaries' business model[6] and the potential risks involved (e.g. privacy-related risks). It is likely that FIDA will put additional weight on the banks' current business model, and this at a time when they are called to finance twin transitions (i.e. combined implementation of digitalization and sustainability), face the advent of the digital euro and are required to implement a great number of new rules (i.e. prudential, financial markets, sustainable finance, payments) that entail substantial investments.
- Finally, the proposed framework does not assess risks that could stem from data transfer to third countries.
- GDPR: This analysis appears to be incomplete, as also confirmed by the European Data Protection Supervisor analysis dated 22 August 2023[7]. While clients' consent is acknowledged to be necessary, there is no further provision on the required granularity of approvals or on the protection of clients who do not wish to consent to data sharing.
- Quantitative impact assessment of the investments required to implement data sharing vs demand by customers. The experience gained from the implementation of the updated PSD2 shows that there has been a negligible uptake by clients of the new services provided by Account Information Service Providers"). Thus, there is currently very limited demand from the market for sharing data. On the other hand, the implementation of PSD2 has required high investments that banks are incurring in order to be compliant with the directive. In the same vein, the mandatory approach of data sharing adopted by FIDA appears disproportionate if there is the concrete risk that banks will not see a return on their investments. A market-driven approach whereby the industry could develop products and services according to the real needs of their customers should be preferred.
- Impact of emerging new technologies, such as generative artificial intelligence (AI) or synthetic data. There is a risk that new technologies in the data space could overtake the FIDA proposal. The impact analysis does not yet consider this. Such technologies could be exploited, for example, by non-EU financial information services providers (also potentially held by a BigTech firm or "gatekeeper" as defined in the DMA) who could use the EU customer data under the FIDA scheme to create synthetic data copies or to enrich Large Language Models – Generative AI services with EU contextual content. Therefore, while such a scenario might not directly lead to a violation of EU data privacy rules, it could enable exploitation of EU financial sector data. In particular, non-EU actors could enrich their analysis capabilities and offer new targeted products, such as innovative investment advice tailored to EU customer data. This presents a lack of protection for EU customer data and might also inadvertently create an unlevel playing field for EU actors.

Comments on specific aspects

The EFMLG would also like to raise the following key concerns related to the proposal.

1. Unlevel playing field

In the absence of any reciprocity, the proposal could unfairly expose the EU industry to the competition from third country-based providers. In fact, EU banks would not be allowed to offer equivalent services outside the EU if a similar regulatory framework is not in place there as is currently the case. The proposal would give non-EU Big Tech firms access to data on EU firms and citizens, which, together with the vast amount of data they already have access to (through the use of innovative technologies like generative AI, and the experience gained in the social media space), could be the ultimate real winner.

Moreover, the proposal also deepens the asymmetry in data sharing (introduced by PSD2) with respect to other sectors. Only large digital platforms (under the DMA) and providers of connected physical objects (under the Data Act) are subject to similar data sharing obligations, while in the case of the DMA, it is highly uncertain how Big Techs will implement their own (less detailed) obligations. Given that boundaries between traditional

[6] As required by the Council conclusions on the Commission Communication on a Retail Payment Strategy for the EU (March 2021).
[7] See opinion 38/2023 by the European Data Protection Supervisor (EDPS) dated 22 August 2023.

sectors are blurring in the digital economy, customer data sharing should be regulated through a horizontal approach, rather than sector by sector. This would create greater opportunities for data-driven innovation (e.g. by facilitating the combination of different types of data) and preserve a competitive level playing field.

2. Definition of customer data

The definition of 'customer data' in Article 3(3) of draft FIDA[8] appears too wide. In particular, it refers not only to personal and non-personal data but also includes contextual data generated as a result of customer interaction with the financial institution (e.g. appropriateness/suitability assessments or creditworthiness). In our view, only standardized raw data should be subject to the sharing obligation, while leaving aside inferred and derived data, data resulting from internal analyses and assessments, as well as data of sensitive commercial nature and trade secrets. The prerequisite to data sharing should be data standardization, ideally related to data categories already standardized, e.g. for regulatory reporting or disclosure purposes. Unstructured not-standardized data should not be subject to data sharing under FIDA.

Consequently, data collected for the suitability and appropriateness assessments under MiFID should be excluded from the scope of FIDA, because the assessment process is not standardized and may also differ depending on the context. Further, the MiFID questionnaire and the interaction with a customer are the result of a specific process and know-how that allows one bank to differentiate itself from the other. A similar reasoning could also be applied to the creditworthiness assessment use case, which additionally is based on different approved regulatory models and will therefore not be comparable across the industry. In addition, the sensitivity of a creditworthiness assessment from a client perspective is another reason to exclude it from the scope of customer data in Article 3(3). This view also appears to be supported by the recent decision of the European Court of Justice of 7 December 2023, whereby the Court made clear that creditworthiness assessments could not be made based purely on automated information and that "[…] *such measures must include, in particular, the obligation for the controller to use appropriate mathematical or statistical procedures, implement technical and organisational measures appropriate to ensure that the risk of errors is minimised and inaccuracies are corrected, and secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and prevent, inter alia, discriminatory effects on that person.* ***Those measures include, moreover, at least the right for the data subject to obtain human intervention on the part of the controller, to express his or her point of view and to challenge the decision taken in his or her regard***" (emphasis added)[9].

Moreover, the definition of 'data' should be clear and provide legal certainty for the data holder, data user and customers. Therefore, Article 2(1) should be amended accordingly, i.e., it should only include clearly identifiable data collected in a standardized manner which may benefit the comparability of products and services. The provision should also exclude inferred/derived data as well as certain commercially sensitive data (intellectual property).

With regards to the dashboard proposed, it should be clear that third party access to all personal and business specific data of the customers should be subject to their prior, clearly documented and unambiguous specific consent (opt-in-system). It should be avoided that customers have to actively prevent data-flow to third parties.

As data generated by data holders, e.g. rating data, is based on methodologies which themselves are subject to business secrecy, such data must be excluded from data sharing obligations. This is because Financial Information Services Providers (FISPs) could – based on output-data – restructure the modelling hypothesis. This could be the case also for other data generated by data-holders, e.g. if data could be used to replicate business strategies, etc.

3. Data in scope

[8] Unless otherwise provided, all references to Articles in this letter are meant to refer to the Articles of draft FIDA.
[9] See Judgment of 07/12/2023 in case C-634/21, Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany)— OQ v Land Hesse, SCHUFA Holding (Scoring), para. 66.

Article 2 of draft FIDA sets forth an extensive list of data categories subject to the sharing obligation. We are concerned that the scope of the proposed mandatory customer data access rights covers a wide range of financial services products, with a potentially large amount of data that is sensitive for the customer and the data holder, without clear predictions on the benefit or an appreciation of the risks.

Generally, customer data should be restricted to data from highly standardized products, e.g. for retail customers, excluding data from corporate and institutional customers with highly individualized products. In any case, it seems that retail is the main focus. Including other customer groups would potentially need specific rules, as the data structure could be very different. In addition, structuring data on individualized products could also be very costly and challenging. in view of business secrecy of the data holders and customers.

Based on the experience with the PSD2 and taking into consideration the considerable investments needed to adhere to the proposed FIDA, also in light of the absence of a quantitative impact assessment of the proposal, we believe that the policy makers should adopt a staggered approach, by starting with a first set of selected data. Such an approach would enable data holders to assess the market take up and avoid investments that cannot be recovered.

Finally, we are concerned about the proposed mandates to EBA and EIOPA to develop guidelines on the use of personal data within the scope of FIDA for the purposes of assessing creditworthiness and pricing of life and health insurance products. These new guidelines might limit innovation and the possibility to differentiate from competitors. In addition, it is not clear whether those guidelines would also apply to the use of data that is within the scope of FIDA but is already held by the bank without having been accessed from a third party.

4. Financial Information Services Providers - FISPs

Entities interested in accessing customer data held by data holders are required to be licensed and subject to supervision. Such requirements are certainly positive, as customer data sharing is allowed within a perimeter of regulated and supervised entities.

In our view, FISPs should be subject to stringent supervision by financial markets authorities. The proposed regulation should focus on defining a set of comprehensive duties for FISPs whereas the requirements proposed under the draft FIDA seem too generic. We would encourage policy makers to focus on this topic in more detail. To establish a fair level playing field between data holders and data users (i.e. FISPs), the latter should be subject to the same data related requirements as the data holders, e.g. in terms of supervisory requirements, BCBS 239[10], DORA[11] and related ESA's requirements. Also, it should be clear that the same supervisory activities as with financial institutions should apply to FISPs, e.g. on- and off-site supervision, data reporting and disclosure, ad-hoc data requests, fire-drill exercises, etc.

4.1 Clarity on Financial Information Services

In our view, certain aspects related to FISPs need further consideration. In particular, FISPs are described in Article 3 as data user authorized under Article 14 to access customer data listed in Article 2(1) for the purpose of provision of financial information services. However, it is not clear what "financial information service" means. This is particularly relevant when considered in conjunction with recital 31, where it is stated that "FISPs would provide financial products and services to customers in the Union and would access data held by financial institutions […]". In our view a) FISPs should not be allowed as such to provide financial products and services unless they are duly licensed; b) recital 31 should be amended by deleting the reference to the provision of financial products and services to ensure that FISPs are authorized only for providing financial information services.

[10] Basel Committee on Banking Supervision's standard No. 239.
[11] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

4.2 Third country FISPs

Article 13 requires FISPs established outside of the EU to appoint a legal representative in one of the member states from where the FISP intends to access financial data.

The legal representative may be held liable for non-compliance with the obligations under FIDA, without prejudice to the liability and legal actions that could be initiated against the FISP.

We believe that the proposed regulation should further clarify:

i) how the organizational requirements would apply in such a case to the FISP;
ii) how NCAs will be able to exercise effective supervision on FISPs established in third countries in case they are not subject to licensing and supervisory requirements in their country of origin.

In our view FIDA should require third country FISPs to have a direct legal presence – a subsidiary or a branch - to obtain the authorization. A legal representative is not sufficient. They should be subject to the same level of supervision under same conditions (compliance with GDPR, DORA and other relevant legislation).

FIDA should address such aspects from a level playing field and customer protection perspective.

As a more general point of concern, there is lack of reciprocity in the sense that third country FISPs are granted extensive access to EU customers' financial data without there being any equivalent possibility for EU firms. Therefore, it should only be possible for third country FISPs to access data in case of reciprocity and effective judicial redress in terms of liability in this third country. It should also be possible for an NCA to withdraw the license for a FISP if reciprocity or effective judicial redress is no longer provided. Reciprocity should not only cover access to financial data in the respective third country by EEA financial providers but should also mean that FISPs are supervised under a comparably strict supervisory regime as within the EEA.

4.3 Treatment of FISPs vs data holders: FISPs should be considered as data holders

Article 6 provides that (i) financial institutions and FISPs can access and use data upon customers' consent and to perform the service explicitly requested by them, and (ii) data holders are required to share data upon their customers' request. We observe that there is no equivalent requirement for FISPs not belonging to the financial services area (i.e., those listed in Art. 2(2)), as they are considered only as data users. However, we believe that these FISPs should also be considered as data holders and therefore required to share their data. For this reason, there should be a **reciprocity requirement in the licensing of third-parties**, pursuant to which firms from outside of the financial sector (e.g. e-commerce, telcos) should also make their own customer data accessible under similar conditions in order to be authorized as a FISP and thereby be able to access financial data. Otherwise, those firms would be able to combine their own customer data with financial data accessed under FIDA, whereas financial entities would not be able to do so due to the lack of accessibility to non-financial customer data.

In our view such reciprocity requirement would ensure a symmetric approach and a level playing field among all entities holding data, in particular in the case where Big Tech firms would apply for a FISP authorisation.

In our view, EEA regulated financial entities, such as credit institutions, should be granted a FISP status under the general supervision regime.

5. Risks posed by Big Tech firms and "gatekeepers"

The risk that Big Tech firms and "gatekeepers" (the latter as defined in Articles 2(1) and 3 of the DMA) may gain a dominant position in the financial space because of their access to financial data should be considered. It is noted that under the DMA, such entities cannot combine data acquired from third party platforms with data they already have (see Article 5(2)(b) of the DMA) and cannot cross-use personal data from the relevant core

platform service in other services provided separately by the gatekeeper (see Art. 5(2)(c) of the DMA). FIDA should not only align with the DMA in this respect but also adopt a more forward-looking approach in light of emerging new technologies (such as generative AI and synthetic data) that could otherwise make its data sharing provisions rapidly obsolete.

As indicated earlier, these technologies could be exploited by a non-EU FISP (also potentially held by Big Tech firms and "gatekeepers") to use the EU customer data under the FIDA scheme to create synthetic data copies or to enrich Large Language Model – Generative AI services with EU customer data (contextual content). In this case, while such an activity might not strictly speaking violate, for example, EU data privacy rules, by exploiting EU financial sector data Big Tech firms or financial services competitors located in other jurisdictions could enrich their analysis capabilities and offer new targeted products, such as for example innovative investment advice, already tailored on the basis of EU customer data.

6. Financial data sharing schemes - FDSS

Timeline of implementation: Article 9 sets forth a challenging 18-month period for data users and data holders to become members of a financial data sharing scheme. Based on the experience gained with open banking, such timeline is far too short for setting up schemes covering such a large range of new data sets. Hence, we suggest setting a more realistic timeline of 3 years, phased in three stages: set up, development and implementation.

In fact, developing FDSSs requires adequate time in order to integrate them into an architectural system (e.g. in terms of authentication methods, functional settings, pricing methodologies etc.) for third party access that is coherent with those already developed for the open banking. Such an approach would avoid cost duplications.

An adequate implementation time would also give time to the market to explore and develop use cases that meet consumers' needs, thus optimizing investments.

As to how FDSSs are supposed to look, the proposal seems to leave it to the market. .In particular, the proposal is silent and provides no clarity as to whether FDSSs should be set up as pan-European schemes or national ones, eventually to be made interoperable with each other at a certain stage, and whether they should be single-product or multi-product. For the sake of proportionality, since developing such schemes will imply considerable investments, there is a need to provide guidance and clarity to the market, to avoid unnecessary costs before the data holders start developing such entities.

Article11 empowers the Commission to issue a delegated act in case a financial data sharing scheme is not developed and there is no realistic prospect of such scheme being set up within a reasonable amount of time. We believe that the conditions under which such delegation is activated are not adequately phrased and circumscribed, in particular with reference to the „reasonable amount of time" and to the difficulties faced by the market in developing such schemes. , The overarching powers established by Article 11 may serve as a disincentive for data holders to invest in scheme development, if there is a risk that the work done could be jeopardized because it does not fit in the time frame or the conditions of the Commission. We would suggest deleting this provision from the text and reconsider the approach.

7. Liability and dispute resolution

The proposal provides little on the liability regime, except for Article10(1)(i) that leaves the task of regulating the allocation of liability within the scheme to the contractual arrangements underpinning the FDSS. In the same vein, the obligations and liabilities for data users in terms of data security and data governance are unclear. We consider that the regulation should introduce a clear liability regime between data holders and data users vis à vis customers sharing data, for cases like data breaches, data loss or illegal use of data. It should also introduce a setup of dispute resolution mechanisms mirroring that in Article10(1)(j) for members of the FDSS.

In respect of data quality considerations, it should be clarified that data holders' liability should be limited to standard data quality checks. It should be clear that data holders cannot be made liable on a single-case basis if standard data quality checks are in place.

8. Compensation

Any data sharing by data holders with FISPs should be fully and fairly compensated by FISPs. All related costs should enter the calculation methodology, relating to data generation, data preparation, data standardization, data quality measures, data maintenance, creation and maintenance of the interfaces and creation and maintenance of customer dashboards by the data holders. Moreover, it should be clear that any profit generated by the FISPs should be shared with the data holders. Only if this pre-requisite of cost transparency and fair sharing of profits is fulfilled, should data sharing be facilitated.

We welcome the fact that – drawing from the lessons learnt from open banking – Article 10 (1)(h) has introduced the concept of compensation to be established in the FDSS. This is certainly a good step in the right direction. However, by stating that "reasonable compensation should be directly related to the making of data available to the data user", the proposal fails to acknowledge that data sharing is not limited to the setup of the technical interface for data sharing. It should also include all the steps leading to data sharing, such as their collection, generation, quality data assurance etc. that will enable FISPs to make good use of the data and make profitable business out of it.

This concept has been acknowledged in Article 9(1) of the Data Act, which states that "(…) any compensation agreed between a data holder and a data recipient (…) shall be non-discriminatory and reasonable and may include a margin." Moreover, it states that the data holder and recipient should take into account i) "the costs incurred for making the data available, including in particular the costs necessary for the formatting of the data, dissemination via electronic means and storage; ii) the investment in the collection and production of data, where applicable, taking into account whether other parties contributed to the obtaining, generating or collecting the data in question". Since recital 47 of FIDA provides a link to the Data Act, we think that in order to ensure a consistent approach in the data sharing space, the wording of Article 10(1) should be amended accordingly.

Moreover, we caution against the cost cap introduced in Article 10(1) h v), that aims at gearing compensation towards the lowest levels prevalent in the market. We see a clear risk of a race to the bottom for technical design and functionalities due to that compensation principle. Therefore, we would recommend deleting this reference.

9. Security and fraud

While we welcome that FISPs will be required to comply with DORA, i.e. with a high level of operational security, we are concerned that there is the risk that data holders and data users apply different levels of standard to the same type of data and services, since banks are required to comply with more stringent rules (see, for example, the Basel principles for effective risk data aggregation and risk reporting (BCBS239)) in terms of data governance, information security, data aggregation and risk reporting.

Additionally, wide dissemination of personal data will be critical, given that the more data are circulated on different interfaces open to countless subjects (in particular non-EU entities or groups of entities), the greater the risk of data breaches and social engineering-based cyber-attacks. By opening up customers' data to third parties, new kinds of fraud are likely to emerge, like social engineering and scams. In such a new environment, consumers may find it more difficult to detect fraud, their consent to access their data may be obtained without their knowledge or they may become recipients of dubious offerings.

Moreover, the sharing of data that a consumer sees as referable to the bank may increase the risk of fraud and scams leveraging on the trust relationship between a bank and its customers. In this case, the reputational

risk for the banks is also increased given the difficulties for customers to consider other parties liable for data he/she initially shared only with his/her bank. In our view, banks should only be held accountable for the safety of data in their own sphere. Therefore, a clear liability regime between data holders and data users in case of data breaches should be defined.

In any case, misuse of data by FISPs should give customers and data holders the right to immediately cut off any data flows at any point in time.

For this reason, we believe that a deeper and more thorough analysis on possible fraud schemes and how to prevent them in the financial data schemes, is also warranted.

10. Permission dashboards

We believe that permission dashboards can help customers control the flow of their data in a secure and trusted way. However, the regulation should not be too prescriptive with respect to the manner in which the service is provided nor oblige data holders to provide information on the agreement between the data user and the customer. It should rather leave enough room for entities to develop the interfaces that best cater to their users' needs. In that context, we believe that a number of requirements are challenging, if not impossible, to meet and should, therefore, be removed (i) inform the data user of the purpose of the permission granted; (ii) show 'the categories of data being shared', and (iii) allow a customer to re-establish any withdrawn permission.

In addition, it should be clarified that the dashboard should only be offered to customers using online interfaces. Imposing an obligation to offer dashboards for users who do not use online banking tools would not only be disproportionate but also challenging to develop.

We also think that the implementation of the dashboards under FIDA should be aligned with the requirements foreseen in the future Payment Services Regulation (PSR), to facilitate a uniform customer experience and allow data holders to leverage investment and avoid duplication of costs. Given that the two provisions are almost identical, it is suggested that a single permission dashboard is created which meets the requirements of both FIDA and the PSR.

The EFMLG remains at your disposal for any assistance or support you may need on this matter. Please keep the EFMLG informed on the above topics.

Yours faithfully,

Fernando Conlledo

Vice Chairman of the EFMLG